(12)特許協力条約に基づいて公開された国際出願

10/517258

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年12月24日 (24.12.2003)

PCT

(10) 国際公開番号
WO 03/107193 A1

(51) 国際特許分類[7]: G06F 12/14, 1/00

(21) 国際出願番号: PCT/JP03/07541

(22) 国際出願日: 2003年6月13日 (13.06.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-174883 2002年6月14日 (14.06.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 中井 勝博 (NAKAI,Katsuhiro) [JP/JP]; 〒669-1321 兵庫県 三田市 けやき台４－４３－４ Hyogo (JP). 難波 剛 (NANBA,Tsuyoshi) [JP/JP]; 〒573-1118 大阪府 枚方市 楠葉並木２－２４－１６ Osaka (JP). 平野 雄久 (HIRANO,Takehisa) [JP/JP]; 〒562-0022 大阪府 箕面市 粟生間谷東６－７－９ Osaka (JP). 手塚 智明 (TEZUKA,Tomoaki) [JP/JP]; 〒533-0021 大阪府 大阪市 東淀川区下新庄２－１２－２１－３０１ Osaka (JP).

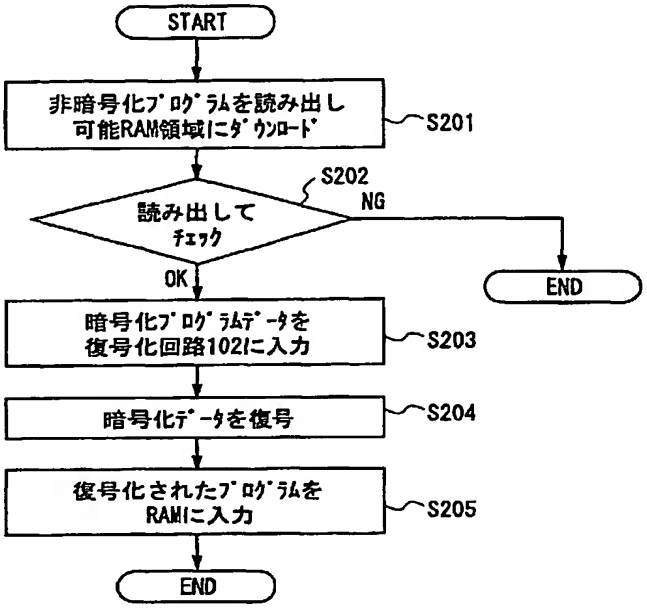
(74) 代理人: 早瀬 憲一 (HAYASE,Kenichi); 〒532-0003 大阪府 大阪市 淀川区宮原３丁目４番３０号 ニッセイ新大阪ビル１３階 早瀬特許事務所 Osaka (JP).

(81) 指定国 (国内): CN, JP, US.

[続葉有]

(54) Title: SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE, DATA STORAGE VERIFICATION DEVICE, AND DATA STORAGE VERIFICATION METHOD

(54) 発明の名称: 半導体集積回路装置、データ記憶検証装置およびデータ記憶検証方法



S201...READ OUT NON-ENCRYPTED PROGRAM AND DOWNLOAD IT INTO A POSSIBLE RAM AREA
S202...READ OUT AND CHECK
S203...INPUT ENCRYPTED PROGRAM DATA IN DECRYPTING CIRCUIT 102
S204...DECRYPT THE ENCODED DATA
S205...INPUT THE DECRYPTED PROGRAM INTO RAM

(57) Abstract: A semiconductor integrated circuit device (100) for downloading a program of a processing unit such as a DSP and a CPU from outside. When a rewrite program which is secret information not to be leaked to a third person is downloaded in a semiconductor integrated circuit (109), it is possible to check whether the rewrite program has been correctly downloaded while maintaining the secrecy. The semiconductor integrated circuit device includes a circuit for verifying the content of the downloaded rewrite program and/or a program for verifying the content of the downloaded rewrite program.

(57) 要約: DSPやCPUなどの演算処理ユニットのプログラムを外部からダウンロードする半導体集積回路装置(100)において、半導体集積回路(109)内にダウンロードした、第三者に漏洩したくない機密情報である書き換えプログラムを、その機密を保持しながら該書き換えプログラムが正しくダウンロードできたか否かの確認を可能とする半導体集積回路装置を提供する。ダウンロードした書き換えプログラムの内容を検証する回路、及び/またはダウンロードした書き換えプログラムの内容を検証するプログラムを備える。

WO 03/107193 A1

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

半導体集積回路装置，データ記憶検証装置およびデータ記憶検証方法

技術分野

本発明は半導体集積回路装置，データ記憶検証装置およびデータ記憶検証方法に関するものであり、特に、内容が第三者へ漏洩したくない機密情報であるプログラムの保護、すなわちその機密性を維持しながら、ダウンロードが確実に実行できたか否かを容易に確認できるようにしたものに関する。

背景技術

ＤＳＰ（Digital Signal Processor）やＣＰＵなどの演算処理ユニットを含む半導体集積回路において、演算処理ユニットのプログラムは、コスト面やプログラムの機密性を保つという点においてはＲＯＭとしてプログラムを格納することが有利となる。しかしながら、ＲＯＭなどの書き換え不可能な手段でプログラムを保持した場合、仕様変更やプログラム自身の不具合に柔軟な対応が取りにくい。このような回路の開発における容易さなどの点から、プログラムを半導体集積回路内部に格納する手段を、ＲＡＭなどの書き換え可能な手段として所有することがある。このような構成を持つ回路においては、ＤＳＰやＣＰＵのような信号処理・機器の制御を担う演算処理ユニットなどに必要なプログラムを事前に書き換え可能なＲＡＭなどの指定領域にダウンロードする必要があった。なお、本明細書において、ダウンロードとは、データやプログラムを、半導体集積回路の内部にロードする、ことを意味するものとする。

しかし、ＤＳＰやＣＰＵなどの演算処理ユニットのプログラムを外部からＲＡＭにダウンロードする半導体集積回路においては、プログラムを半導体集積回路内部にＲＯＭで持っている場合よりもプログラムの内容が第三者に漏洩する危険が高いという欠点を有していた。

例えば、半導体集積回路外部に保持するプログラムが、著作権保護を目的として策定されたウォーターマーク（電子透かし）を検出するためのプログラムのよ

うな場合、プログラムの内容が悪意を持った第三者に漏洩したことによって、著作権保護のための仕組みを無効化される恐れがあるため、プログラム自身を保護する必要がある。

この場合、半導体集積回路内にダウンロードするプログラムを予め暗号化させて、該半導体集積回路内で復号化させることにより、プログラム自身を保護することが考えられる。

しかしながら、この予め暗号化したデータ、及び非暗号化データも含めて半導体集積回路内の書き換え可能な領域にダウンロードしたプログラムデータが正しく格納できたか否かを、機密性を保持しながら確認することは困難である。

本発明はこのような問題を解決するためになされたものであり、機密性を要するプログラムデータを外部に漏らすことなく、正しくダウンロードできたか否かを確認できる半導体集積回路装置，データ記憶検証装置およびデータ記憶検証方法を提供することを目的とする。

発明の開示

上記問題を解決するために、本発明の請求の範囲第１項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第２の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、上記第２の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第１の格納手段からの上記書き換えプログラムを、上記第２の格納手段の外部読出し不可能領域に格納するようにしたものである。

これにより、例えばダミーデータなどを、上記第２の格納手段の読み出し可能

な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、半導体集積回路内に正しく上記書き換えプログラムが格納されたかどうかを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第２の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えたものである。

これにより、上記第２の格納手段に格納された特定部分のみを読み出して、該特定部分を検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３項に記載の半導体集積回路装置は、請求の範囲第２項に記載の半導体集積回路装置において、上記制御回路は、上記第２の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するものとしたものである。

これにより、上記第２の格納手段の特定のアドレスのみを読み出して、該特定のアドレスのデータを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第４項に記載の半導体集積回路装置は、請求の範囲第２項に記載の半導体集積回路装置において、上記制御回路は、上記第２の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとしたものである。

これにより、上記第２の格納手段の特定のビットのみを読み出して、該特定のビットのみを検証することにより、上記書き換えプログラムが半導体集積回路内

に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第５項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、上記第２の格納手段に格納した上記書き換えプログラムの一部を実行するものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第６項に記載の半導体集積回路装置は、請求の範囲第５項に記載の半導体集積回路装置において、上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである。

これにより、例えば、上記第２の格納手段に格納された上記書き換えプログラムの先頭プログラムと最終プログラムとを実行した場合、該書き換えプログラムが最後まで正しく格納できたかを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第７項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第１の格納手段から上記第２の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えたものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第８項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、上記第２の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、上記第２の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行うものである。

これにより、接続切り換え手段にて演算処理ユニットのプログラム入力またはデータ入力を切り替えて、上記書き換えプログラムのデータを取り込んで、例えば該書き換えプログラムデータのチェックサムなどをとって、予め決めておいた値と比較することが可能になるので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密を保持しながら確認することができる。

また、本発明の請求の範囲第９項に記載の半導体集積回路装置は、請求の範囲第８項に記載の半導体集積回路装置において、上記第２の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとしたものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半

導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

また、本発明の請求の範囲第１０項に記載の半導体集積回路装置は、請求の範囲第９項に記載の半導体集積回路装置において、上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用するものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

また、本発明の請求の範囲第１１項に記載の半導体集積回路装置は、請求の範囲第８項に記載の半導体集積回路装置において、上記第２の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次２分割した構成とし、該２分割した各々の領域に同じプログラムデータを格納するものであり、上記チェックプログラムは、上記２分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、前回の判定結果が正しいと判定されたときに、前回２分割した領域の一方の領域を、プログラムが格納されていない領域としてさらに２分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、上記第２の格納手段に格納すべきプログラムすべてを順次格納するものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

また、本発明の請求の範囲第１２項に記載の半導体集積回路装置は、請求の範

囲第１１項に記載の半導体集積回路装置において、上記第２の格納手段は、該第２の格納手段の上記書き換えプログラムが格納されていない領域を順次２分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとしたものである。

これにより、例えば、第２の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第２の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

また、本発明の請求の範囲第１３項に記載の半導体集積回路装置は、請求の範囲第１２項に記載の半導体集積回路装置において、上記一意に得られるデータが、該プログラムデータの反転データであるものとしたものである。

これにより、例えば、第２の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第２の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

また、本発明の請求の範囲第１４項に記載の半導体集積回路装置は、請求の範囲第８項ないし第１３項のいずれかに記載の半導体集積回路装置において、上記チェックプログラムを予め格納したＲＯＭ（Read Only Memory）を備え、上記ＲＯＭにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行うものである。

これにより、上記チェックプログラムの転送誤り等により、チェックプログラムが機能しなくなるのを防ぎ、上記第２の格納手段に上記書き換えプログラムが正しく格納できたか否かを確認するチェックプログラムを安定的に提供することができる効果がある。

また、本発明の請求の範囲第１５項に記載の半導体集積回路装置は、請求の範囲第１項ないし第１４項のいずれかに記載の半導体集積回路装置において、上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を

備え、上記第１の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第２の格納手段に復号化した上記書き換えプログラムを格納するものである。

これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第１６項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第１の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第２の格納手段に転送する復号化手段と、上記第２の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、上記暗号化手段で暗号化された書き換えプログラムと上記第１の格納手段に保持している暗号化された書き換えプログラムとを比較するものである。

これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第１７項に記載の半導体集積回路装置は、請求の範囲第１１項ないし第１３項、及び第１６項のいずれかに記載の半導体集積回路装置において、上記第２の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第１の格納手段に保持した書き換えプログラムを修正可能としたものである。

これにより、第２の格納手段において正しく格納できなかった箇所を使用しないように書き換えプログラムを修正して書き込むので、メモリを有効に活用することができる。

また、本発明の請求の範囲第１８項に記載の半導体集積回路装置は、請求の範囲第１項ないし第１７項のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたものである。

これにより、書き換えプログラムを半導体集積回路装置外部に有する場合においても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる。

また、本発明の請求の範囲第１９項に記載のデータ記憶検証装置は、任意のデータを外部からアクセス可能な領域に記憶させる手段と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する手段と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる手段とを備えた、ことを特徴とするものである。

これにより、例えばダミーデータなどを、上記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく上記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２０項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な領域に記憶させる手段と、前記機密データの特定部分を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データの特定部分のみを読み出して、該特定部分を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２１項に記載のデータ記憶検証装置は、プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる手段と、前記記憶されたプログラムを実行させ、結果を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれ

ているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２２項に記載のデータ記憶検証装置は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第１の手段と、前記検査プログラムを実行させ、結果を外部に出力する第２の手段と、前記第２の手段の終了後、前記機密プログラムを実行させる第３の手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

また、本発明の請求の範囲第２３項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な領域に記憶させる手段と、前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、前記演算の結果を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２４項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な第１の領域に記憶させる第４の手段と、機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域に記憶させる第５の手段と、前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の手段とを備えた、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な第１の領域に格納するとともに、その機密データの一部である検査プログラムを第２の領域に格納し、この検査プログラムを用いて検査を行い、その検査結果を外部に出力して、第１の

領域の機密データの正当性を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２５項に記載のデータ記憶検証装置は、請求項２４記載のデータ記憶検証装置において、前記第６の手段の終了後に前記第１の領域の命令に制御を移す第７の手段をさらに備えた、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認した後に、本来の機密データに含まれる命令の実行に移ることができる。

また、本発明の請求の範囲第２６項に記載のデータ記憶検証装置は、請求項２４記載のデータ記憶検証装置において、前記第５の手段は、前記第１の領域に記憶されている機密データ内に存在する命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データ内に存在する命令により行うことができる。

また、本発明の請求の範囲第２７項に記載のデータ記憶検証装置は、請求項２４記載のデータ記憶検証装置において、前記第５の手段は、第３の領域に前記第４の手段による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データを格納するより前に格納した命令により行うことができる。

また、本発明の請求の範囲第２８項に記載のデータ記憶検証装置は、機密データを復号する手段と、前記復号されたデータを外部からアクセス不可能な領域に記憶させる手段と、前記記憶されたデータを暗号化する手段と、前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する手段とを備えた、ことを特徴とするものである。

これにより、いったん復号して外部からアクセス不可能な領域に格納した機密

データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第２９項に記載のデータ記憶検証装置は、機密プログラムを外部からアクセス不可能な領域に記憶させる手段と、前記記憶されたプログラムを読み出す手段と、前記読み出されたプログラムを命令単位で正当性を判定する手段と、正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域において空いている領域に記憶させる手段と、前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる手段と、正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる手段とを備えた、ことを特徴とするものである。

これにより、機密プログラムを外部からアクセス不可能な領域に格納し、その格納したプログラムを読み出し命令単位で正当性を判定し、正当でないと判定された命令に対しては外部からアクセス不可能な領域の空き領域に格納した正当な命令にジャンプすることにより、機密プログラムを格納する際にその一部に正しく格納できていない命令が含まれていても、空き領域に格納した正しい命令に置換してこれを実行することができる。

また、本発明の請求の範囲第３０項に記載のデータ記憶検証方法は、任意のデータを外部からアクセス可能な領域に記憶させる工程と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる工程とを含む、ことを特徴とするものである。

これにより、例えばダミーデータなどを、前記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく前記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３１項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な領域に記憶させる工程と、前記機密データの特定

部分を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データの特定部分のみを読み出して、該特定部分を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３２項に記載のデータ記憶検証方法は、プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる工程と、前記記憶されたプログラムを実行させ、結果を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３３項に記載のデータ記憶検証方法は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第１の工程と、前記検査プログラムを実行させ、結果を外部に出力する第２の工程と、前記第２の工程の終了後、前記機密プログラムを実行させる第３の工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

また、本発明の請求の範囲第３４項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な領域に記憶させる工程と、前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、前記演算の結果を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、前記機密データが正しくダウンロードできたか

否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３５項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な第１の領域に記憶させる第４の工程と、機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域に記憶させる第５の工程と、前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の工程とを含む、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な第１の領域に格納するとともに、その機密データの一部である検査プログラムを第２の領域に格納し、この検査プログラムを用いて検査を行い、その検査結果を外部に出力して、第１の領域の機密データの正当性を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第３６項に記載のデータ記憶検証方法は、請求項３５記載のデータ記憶検証方法において、前記第６の工程の終了後に前記第１の領域の命令に制御を移す第７の工程をさらに含む、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認した後に、本来の機密データに含まれる命令の実行に移ることができる。

また、本発明の請求の範囲第３７項に記載のデータ記憶検証方法は、請求項３５記載のデータ記憶検証方法において、前記第５の工程は、前記第１の領域に記憶されている機密データ内に存在する命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データ内に存在する命令により行うことができる。

また、本発明の請求の範囲第３８項に記載のデータ記憶検証方法は、請求項３５記載のデータ記憶検証方法において、前記第５の工程は、前記第３の領域に前記第４の工程による記憶の実行以前に記憶された命令により前記検査プログラム

の記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データを格納するより前に格納した命令により行うことができる。

また、本発明の請求の範囲第３９項に記載のデータ記憶検証方法は、機密データを復号する工程と、前記復号されたデータを外部からアクセス不可能な領域に記憶させる工程と、前記記憶されたデータを暗号化する工程と、前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する工程とを含む、ことを特徴とするものである。

これにより、いったん復号して外部からアクセス不可能な領域に格納した機密データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第４０項に記載のデータ記憶検証方法は、機密プログラムを外部からアクセス不可能な領域に記憶させる工程と、前記記憶されたプログラムを読み出す工程と、前記読み出されたプログラムを命令単位で正当性を判定する工程と、正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域において空いている領域に記憶させる工程と、前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる工程と、正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる工程とを含む、ことを特徴とするものである。

これにより、機密プログラムを外部からアクセス不可能な領域に格納し、その格納したプログラムを読み出し命令単位で正当性を判定し、正当でないと判定された命令に対しては外部からアクセス不可能な領域の空き領域に格納した正当な命令にジャンプすることにより、機密プログラムを格納する際にその一部に正しく格納できていない命令が含まれていても、空き領域に格納した正しい命令に置換してこれを実行することができる。

図面の簡単な説明

第１図は、本発明の実施の形態１における半導体集積回路装置を示す図

第２図は、本発明の実施の形態１における半導体集積回路装置の動作を示すフローチャート

第３図は、本発明の実施の形態２における半導体集積回路装置を示す図

第４図は、本発明の実施の形態２における半導体集積回路装置の動作を示すフローチャート

第５図は、本発明の実施の形態３における半導体集積回路装置を示す図

第６図は、本発明の実施の形態３における半導体集積回路装置を示す図

第７図は、本発明の実施の形態３における半導体集積回路の実行プログラムの一例を示す図

第８図は、本発明の実施の形態４における半導体集積回路装置を示す図

第９図は、本発明の実施の形態５における半導体集積回路装置を示すブロック構成図

第１０図は、本発明の実施の形態５における半導体集積回路装置のＲＡＭ（第２の格納手段）の構成の一例を示す構成図

第１１図は、本発明の実施の形態６における半導体集積回路装置を示すブロック構成図

第１２図は、本発明の実施の形態６における半導体集積回路装置のＲＡＭ（第２の格納手段）１１０６の構成の一例を示す図

第１３図は、本発明の実施の形態６におけるメモリ１１０２内のデータ配置を示す概念図

第１４図は、本発明の実施の形態７における半導体集積回路装置を示すブロック構成図

第１５図は、本発明の実施の形態８における半導体集積回路装置を示すブロック構成図

第１６図は、本発明の実施の形態８における半導体集積回路装置の動作を示すフローチャート

第１７図は、本発明の実施の形態８における半導体集積回路装置のプログラム

の修正を行う一例を示した図

発明を実施するための最良の形態

以下、本発明の実施の形態について、図を用いて説明する。

（実施の形態１）

第１図は、本発明の実施の形態１に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

図において、１００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、例えば１０５は制御用マイコン、１０１はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）である。半導体集積回路１０９は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）１０２と、書き換え可能なＲＡＭ（第２の格納手段）１０８と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ１０７の処理を行う演算処理回路（演算処理ユニット）１０６とから構成される。なお、書き換えプログラムは例えばこれを変更することで演算処理回路１０６に異なる機能を実現させるものである。

また、本発明の実施の形態１に係る半導体集積回路装置において、書き換え可能なＲＡＭ１０８は、半導体集積回路１０９の外部から読み出し可能な外部読出し可能領域１０３と、半導体集積回路１０９の外部から読み出し不可能な外部読出し不可能領域１０４とから構成される。この外部読出し不可能領域１０４は、例えば、外部からのアドレスバスは外部読出し可能領域１０３と同様外部読出し不可能領域１０４に接続するが、外部にデータを読み出す場合はデータバスは外部読出し不可能領域１０４には接続しないスイッチを設けること等で実現できる。

以上のように構成された半導体集積回路装置１００について、第２図のフローチャートを用いてその動作を説明する。

制御用マイコン１０５の制御にしたがい、暗号化されていないデータを書き換え可能なＲＡＭ１０８の外部読出し可能領域１０３に入力する（ステップＳ２０１）。次に、外部読出し可能領域１０３に入力したデータが正しいかを半導体集積回路１０９外部に読み出して制御用マイコン１０５等でチェックする（ステップ

Ｓ２０２）。ステップＳ２０２でチェックした結果が正しい場合は、制御用マイコン１０５の制御にしたがいメモリ１０１の暗号化された書き換えプログラムを復号化回路１０２に入力し（ステップＳ２０３）、復号化回路１０２は、暗号化された書き換えプログラムを復号する（ステップＳ２０４）。次に、ステップＳ２０４で復号化された書き換えプログラムを書き換え可能なＲＡＭ１０８の外部読出し不可能領域１０４に入力する（ステップＳ２０５）。以上の処理により、第三者に漏洩したくない書き換えプログラムの機密性を保ちながら、該書き換えプログラムが正しく格納されているか否かをチェックすることができる。

これは、上述のように暗号化されていないデータを外部から書き込み正しく読み出せたことは、これらを実行する回路に故障が生じていないと考えられるので、書き換えプログラムを外部読出し不可能領域１０４に格納する際にもこれを支障なく行えていると考えられるからである。

なお、書き換え可能なＲＡＭ１０９の外部読出し可能領域１０３に格納するデータは、半導体集積回路装置の内部、及び外部のどちらに用意してもよく、チェック用のデータであればよい。

以上のような、本発明の実施の形態１に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムを書き換え可能なＲＡＭ１０８に入力する場合に、該ＲＡＭ１０８に設けた外部読出し可能領域１０３、及び外部読出し不可能領域１０４のうち、外部読み出し可能領域１０３にチェック用のデータを格納し、該データのチェックの結果が正しいと判定された後、外部読出し不可能領域１０４に該機密情報のプログラムを格納することにより、第三者に漏洩したくない機密情報である書き換えプログラムを格納したＲＡＭ１０８の製造上の欠陥、及び入力するまでの経路のチェックをすることができる。

（実施の形態２）

本発明の実施の形態２に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムの機密性を保ちながら、該書き換えプログラムが半導体集積回路内の書き換え可能なＲＡＭに正しく格納されているかを確認するために、格納した書き換えプログラムの特定部分のみを半導体集積回路に読み出すように制御する制御回路を備えたものである。

第３図は、本発明の実施の形態２に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

図において、３００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、３０１は制御用マイコン、３０３はあらかじめ暗号化された書き換えプログラムを格納しているメモリ（第１の格納手段）である。半導体集積回路３０８は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）３０２と、復号化回路３０２で復号した書き換えプログラムを格納するための書き換え可能なＲＡＭ（第２の格納手段）３０４と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ３０７の処理を行う演算処理回路（演算処理ユニット）３０５と、ＲＡＭ３０４に格納された書き換えプログラムのうち特定アドレスのみ出力するように制御する制御回路３０６とから構成される。制御回路３０６はＲＡＭ３０４の特定のアドレスのみを外部に読み出す機能を有する。

次に、以上のように構成された半導体集積回路装置３００について、第４図のフローチャートを用いて動作を説明する。

暗号化された書き換えプログラムを格納するメモリ３０３からの該書き換えプログラムを復号化回路３０２で復号し（ステップＳ４０１）、該復号化した書き換えプログラムをＲＡＭ３０４に入力する（ステップＳ４０２）。次に、制御回路３０６から、ＲＡＭ３０４に格納されている書き換えプログラムの特定アドレスの読み出しを行い（ステップＳ４０３）、該特定アドレスのプログラムを半導体集積回路３０８外部に読み出してチェックする（ステップＳ４０４）。

以上のような本発明の実施の形態２に係る半導体集積回路装置は、書き換えプログラムをＲＡＭ３０４に格納した後、特定のアドレスのみを半導体集積回路外部に読み出すように制御する制御回路を備え、該読み出された特定アドレスをチェックすることにより、第三者に漏洩したくない機密情報である書き換えプログラムがＲＡＭ３０４に正しく格納されたかどうかを、該書き換えプログラムの機密性を保持しながら判断することができる。

これは、外部に読み出したのが特定アドレスであっても、それが正しい値であれば、書き換えプログラム全体が正しく格納されていると考えられるからである。

なお、本実施の形態２では特定アドレスのみを読み出し可能としたが、特定ビットのみを半導体集積回路外部に読み出すように制御し、該読み出した特定ビットをチェックしても、書き換えプログラムがＲＡＭに格納されたかどうか判断することができる。

（実施の形態３）

本発明の実施の形態３に係る半導体集積回路装置は、第三者に漏洩したくない機密情報の書き換えプログラムが半導体集積回路内の書き換え可能なＲＡＭに正しく格納されているかを判断するために、該半導体集積回路のＲＡＭに格納した書き換えプログラムの一部を実行するものである。

第５図は、本発明の実施の形態３に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

図において、５００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、５０１は制御用マイコン、５０３は、あらかじめ暗号化された書き換えプログラムを格納しているメモリ（第１の格納手段）である。半導体集積回路５０７は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）５０２と、復号化回路５０２で復号化された書き換えプログラムを格納するための書き換え可能なＲＡＭ（第２の格納手段）５０４と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ５０６の処理を行う演算処理回路（演算処理ユニット）５０５とから構成される。

本実施の形態３において、上記あらかじめ暗号化された書き換えプログラムには、ダウンロード後に該書き換えプログラムの一部を実行するプログラム（チェックプログラム）が含まれているものとする。また、チェックプログラムは復号化の際に書換えプログラムに挿入されてもよい。

次に、以上のように構成された半導体集積回路５００について、第６図のフローチャートを用いてその動作を説明する。

メモリ５０３からの暗号化した書き換えプログラムを復号化回路５０２で復号し（ステップＳ６０１）、該復号した書き換えプログラムをＲＡＭ５０４に入力する（ステップＳ６０２）。次に、ＲＡＭ５０４に格納した書き換えプログラムの一

部を実行させ（ステップＳ６０３）、正しいか否かが判断されたら、半導体集積回路５０７外部に正しいか否かを通知する信号を出力する（ステップＳ６０４）。

このとき、実行するプログラムの内容を例えばメモリチェックなどのプログラムにし、該メモリチェックを実行させ、そのチェックの結果が得られたならば、ＲＡＭ５０４に正しくプログラムが格納されているかの判断をより確実に行える。

また、第７図のように、実行するプログラムの内容を、ＪＵＭＰ命令などを実行して非連続領域のプログラムを実行するプログラムにし、例えば、先頭プログラムでメモリチェックのプログラムのアドレスＸＸにＪＵＭＰする命令を実行するとする。そして、先頭プログラムからメモリチェックのプログラムのアドレスＸＸにＪＵＭＰして、メモリチェックを行うようにすることにより、ＲＡＭ５０４に正しくプログラムが格納されているかの判断をより確実に行える。また、先頭プログラムで最終プログラムのアドレスＹＹにＪＵＭＰする命令を実行するとする。そして先頭プログラムから最終プログラムのアドレスＹＹにＪＵＭＰして、該最終プログラムは、該最終プログラムを実行後にアドレス０１に戻るようなプログラムにして、その結果、プログラムが正しく実行されたことを確認することにより、書き換えプログラムがＲＡＭの最後まで書きこまれているかどうかを判断することができ、特に、復号化を１つでも間違うと後段のデータに影響を及ぼす暗号化方式においては、書き換えプログラムが正しく格納されているかをより一層確実に判断できる。

以上のような本発明の実施の形態３に係る半導体集積回路装置は、書き換えプログラムをＲＡＭ５０４に格納した後、該書き換えプログラムの一部を実行し、正しく実行できた場合に信号を出力することによって、書き換えプログラムがＲＡＭに正しく格納できたかどうかを判断することができる。

また、書き換えプログラムを格納したＲＡＭ５０４から、非連続なプログラム領域を順次実行することにより、書き換えプログラムが最後までＲＡＭに正しく格納されたかを確認することが可能になり、ＲＡＭに格納した書き換えプログラムの正誤チェックを、より確実に行うことができる。

（実施の形態４）

本発明の実施の形態４に係る半導体集積回路装置は、第三者に漏洩したくない

機密情報である書き換えプログラムが半導体集積回路内に正しく格納されているかを確認するために、半導体集積回路内のＲＡＭに書き換えプログラムを書き込む際に、転送データを監視する転送監視回路を備え、転送されるデータ単位ごとの算術和をとって結果を保持し、チェックサムなどをとるようにしたものである。

第８図は、本発明の実施の形態４に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

図において、８０１は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、８０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、８０３は制御用のマイコンである。半導体集積回路８１０は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）８０５と、復号化回路８０５で復号化された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）８０６と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ８０７の処理を行う演算処理回路（演算処理ユニット）８０８と、復号化回路８０５から転送されるデータ単位ごとの算術和をとる転送監視回路（転送監視手段）８０９とから構成される。

次に、本発明の実施の形態４に係る半導体集積回路装置の動作を説明する。

以上のように構成された半導体集積回路装置８０１において、あらかじめ暗号化されメモリ８０２に格納された書き換えプログラムを、制御用マイコン８０３の制御のもと、復号化回路８０５をとおして復号しながらＲＡＭ８０６に格納する。この時、同時に、データ転送用のデータパスの一部である復号化回路８０５からＲＡＭ８０６への信号線を転送監視回路８０９が常に監視し、転送されるデータ単位ごとの算術和をとって結果を保持していく。そして、メモリ８０２に格納されたデータのうちあらかじめ決められたデータ量の転送が終了した時点で、転送監視回路８０９に保持されている算術和のデータを読み出し、制御用マイコン８０３において、あらかじめ計算しておいた正しく転送がおこなわれたときのデータの算術和と比較し、同じ値であれば転送が正しくおこなわれたと判断し、その後、本来実行すべき処理を行う。もし、この両者の値が異なっていれば、正しく転送がおこなわれなかったと判断し、メモリ８０２に入っているデータを再

度転送し直すなど、しかるべき処置を施す。

以上のような本発明の実施の形態４に係る半導体集積回路装置は、書き換えるための書き換えプログラムの転送データを監視し、転送されるデータ単位ごとの算術和をとる転送監視回路を備え、該転送監視回路でとった算術和と、あらかじめ計算しておいた正しく転送が行われたときのデータの算術和とを比較するので、第三者に漏洩したくない機密情報である書き換えプログラムを読み出すことなく、正しくダウンロードされたか否かを判断することができる。

なお、本実施の形態４では、データ転送監視回路を用いてチェックサムをとる例を説明したが、チェックサムの代わりにＣＲＣチェック回路、ＥＣＣチェック回路など、データのあるかたまり単位でビット誤りがあるか否かが判定できるものであれば同様の効果を得ることができ、特にこの監視方式を限定するものではない。

（実施の形態５）

本発明の実施の形態５に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムが、半導体集積回路に正しく格納されているか否かを確認するために、演算処理回路のワークメモリから該演算処理回路を動作させることと、ＲＡＭに格納されたプログラムデータを演算処理回路に入力させることとを可能にし、演算処理回路にて、チェックサムなどをとるようにしたものである。

第９図は、本発明の実施の形態５に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

図において、９０１は、暗号化された書き換えプログラムをもつ半導体集積回路装置であって、９０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、９０３は制御用のマイコンである。半導体集積回路９１５は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）９０５と、復号化回路９０５で復号化された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）９０６と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ９０７の処理を行う演算処理回路（演算処理ユニット）９０８と、演算処理回路９０８のワークメモリ

９１１と、ＲＡＭ９０６、及びワークメモリ９１１のそれぞれを、演算処理回路９０８の命令プログラムを読み込むバス９１３、及びデータを入出力するバス９１４に接続できるように切り替える接続切り替え回路（接続切り替え手段）９１２とから構成されている。また、本実施の形態５において、ＲＡＭ９０６と演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続され、ワークメモリ９１１とデータを入出力するバス９１４とが接続される形態を第１の形態とし、また、ＲＡＭ９０６とデータを入出力するバス９１４とが接続され、ワークメモリ９１１と演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続される形態を第２の形態とし、接続切り替え回路９１２は、上記第１、及び第２の形態のいずれかの形態に切り替えるものである。通常の状態では、上記第１の形態を取るものとし、これらの構成により、演算処理回路９０８は、自分自身の命令プログラムを読み込むバス９１３とデータを読み込むバス９１４とは独立しているいわゆるハーバードアーキテクチュアを取ることができ、より高速にコンテンツデータ９０７に対するデータ処理が実行できるものである。

次に、本発明の実施の形態５に係る半導体集積回路装置９０１の動作を説明する。

あらかじめ暗号化されメモリ９０２に格納された書き換えプログラムを制御用マイコン９０３の制御のもと、復号化回路９０５をとおして復号しながらＲＡＭ９０６に格納する。その後、演算処理回路９０８の動作を開始する。このとき演算処理回路９０８は、ＲＡＭ９０６の中の書き換えプログラムに組み込まれた実行ステップに応じて動作する。

また、このＲＡＭ９０６に格納された書き換えプログラムの中に、書き換えプログラムがＲＡＭ９０６に正しく格納できたか否かをチェックするプログラム（チェックプログラム）を予め組み込んでおく。本実施の形態５では、データを入出力するバス９１４上のＲＡＭ９０６のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することによりＲＡＭ９０６に格納されているデータが正しいことを判定するようなプログラムと、正しいと判断された後に接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムとの上記２つのプログラムをマシン語データとして組み込んでおき、さらに、

該組み込んだマシン語データを直接ワークメモリ９１１に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路９１２を第２の形態に切り替えるプログラムとを書き換えプログラムの中に予め組み込んでおく。

そして、動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ９１１に展開するプログラムにより、上記マシン語データである、上記ＲＡＭ９０６に格納されたプログラムが正しいか否かを判定するための上記２つのプログラムがワークメモリ９１１に展開される。その後、上記接続切り替え回路９１２を第２の形態に切り替えるプログラムによって、接続切り替え回路９１２を第２の形態に切り替える。これにより、ワークメモリ９１１と、演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続されるため、演算処理回路９０８はワークメモリ９１１に先ほど展開した上記２つのプログラムのうち、データを入出力するバス９１４上のＲＡＭ９０６のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することによりＲＡＭ９０６に格納されているデータが正しいことを判定するようなプログラムを実行する。これにより、ＲＡＭ９０６に格納されている書き換えプログラムが正しいと判定されれば、上記ワークメモリ９１１に展開した２つのプログラムの残りのプログラムである、接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムを実行することによって、接続切り替え回路９１２は第１の形態に切り替えられ、以後本来実行すべきプログラムを実行する。

次に、ＲＡＭ９０６を第１０図のような構成にした例を説明する。

このＲＡＭ９０６は、第１０図に示すような論理的構成をとるものである。ａ２４００、ａ２４０１、ａ２４０２は、メモリアドレスを示しており、右上がり斜線ハッチをつけたアドレスａ２４００で始まり、アドレスａ２４０１で終わる空間に書き換えプログラムを格納する。また、アドレスａ２４０１で始まり、アドレスａ２４０２で終わる空間には、上記右上がり斜線ハッチをつけたアドレスａ２４００で始まりアドレスａ２４０１で終わる空間に格納されたデータの、たとえばメモリアドレスごとなどのように、あらかじめ決められた単位ごとに対する、たとえばパリティフラグを格納するものとする。

そして、ＲＡＭ９０６に格納する書き換えプログラムの中にあらかじめ組み込んでおくチェックプログラムとして、データを入出力するバス９１４上のＲＡＭ９０６のデータを読み込み、該読み込んだデータの中の１のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムと、さらに前記読み込んだデータに対応するアドレスａ２４０１からａ２４０２の空間に格納されているパリティフラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較してメモリ２４０６に格納された書き換えが正しいか否かを判断するプログラムと、正しいと判断された後に接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムとの上記３つのプログラムをマシン語データとして組み込んでおき、さらに、該組み込んだマシン語データを直接ワークメモリ９１１に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路９１２を第２の形態に切り替えるプログラムとを予め組み込んでおく。

動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ９１１に展開するプログラムにより、上記マシン語データである、上記３つのプログラムがワークメモリ９１１に展開される。その後、上記接続切り替え回路９１２を第２の形態に切り替えるプログラムによって、接続切り替え回路９１２を第２の形態に切り替える。これにより、ワークメモリ９１１と演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続されるため、演算処理回路９０８はワークメモリ９１１に先ほど展開した上記３つのプログラムのうち、データを入出力するバス９１４上のメモリのデータを読み込み、該読み込んだデータの中の１のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムを実行し、次に、前記読み込んだデータに対応するアドレスａ２４０１からａ２４０２の空間に格納されているパリティフラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較してＲＡＭ９０６に格納された書き換えプログラムが正しいか否かを判断するプログラムを実行する。これにより正しいと判断されれば、上記ワークメモリ９１１に展開した３つのプログラムの残りのプログラムである、接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムによっ

て、接続切り替え回路９１２は第１の状態に切り替られ、以後本来実行すべきプログラムを実行する。

このように、ＲＡＭ９０６を上記構成にすることにより、ＲＡＭ９０６に格納した書き換えプログラムが正しく格納されたか否かを確認することができるとともに、書き換えプログラムが正しく格納できていない場合、該正しく格納できていない場所の情報を得ることができる。

なお、ＲＡＭ９０６のアドレスａ２４０１からａ２４０２までの空間に入れるデータは、パリティフラグに限らず、データのあるかたまりで正しいか否かが判定できるものであればよく、現在よく知られているものにＣＲＣチェックやＥＣＣチェックなどがあり、これらを使用しても同様の効果が得られる。

以上のような本発明の実施の形態５に係る半導体集積回路装置は、ＲＡＭ９０６に格納された書き換えプログラムが正しく格納されているかを確認するためのチェックプログラムを演算処理回路のワークメモリ９１１に展開し、接続切り替え回路９１２を切り替えて、ワークメモリ９１１からの命令を可能にし、該ワークメモリ９１１からの命令を受けた演算処理回路にて、チェックサムなどをとることにより、第三者に漏洩したくない機密情報である書き換えプログラムがＲＡＭ９０６に正しく格納されているか否かを、機密性を保持しながら確認することができる。

なお、本発明の実施の形態５に係る半導体集積回路装置では、演算処理回路でチェックサムをとる例を説明したが、チェックサムの代わりにＣＲＣチェック回路、ＥＣＣチェック回路など、データのあるかたまり単位でビットに誤りがあるか否かが判定できるものであれば同様の効果を得ることができる。

（実施の形態６）

本発明の実施の形態６に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路に正しく格納されたか否かの確認を安定して行うために、ＲＡＭに格納された書き換えプログラムが正しいか否かの確認をするためのチェックプログラムを予めＲＯＭに格納して、該ＲＯＭに格納したチェックプログラムによって、上記書き換えプログラムの確認動作を行うものである。

第１１図は、本発明の実施の形態６に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内にダウンロードする例を示す。

図において、１１０１は暗号化された書き換えプログラムをもつ半導体集積回路装置であって、１１０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、半導体集積回路１１１６は、制御用のマイコン１１０３と、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）１１０５と、復号化回路１１０５で復号化した書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）１１０６と、復号化したプログラムの制御手順に従って動作し、コンテンツデータ１１０７の処理を行う演算処理回路（演算処理ユニット）１１０８と、演算処理回路１１０８のワークメモリ１１１１と、ＲＡＭ１１０６、及びワークメモリ１１１１のそれぞれを、演算処理回路１１０８の命令プログラムを読み込むバス１１１３、及びデータを入出力するバス１１１４に接続できるように切り替える接続切り替え回路（接続切り替え手段）１１１２と、演算処理回路１１０８によって実行できるＲＡＭ１１０６に展開された書き換えプログラムが正しいか否かを判定するためのプログラム（チェックプログラム）を格納したＲＯＭ１１１５とから構成され、ＲＯＭ１１１５は、常に演算処理回路１１０８の命令プログラムを読み込むバス１１１３に接続される。また、接続切り替え回路１１１２によって切り替える第１、及び第２の形態は実施の形態５と同様なので説明を省略する。また、実施の形態５と同様、通常の状態では、上記第１の形態を取るものとする。

次に、本発明の実施の形態６に係る半導体集積回路装置の動作を説明する。

まず最初に、あらかじめ暗号化されメモリ１１０２に格納された書き換えプログラムを制御用マイコン１１０３の制御のもと、復号化回路１１０５をとおして復号しながらＲＡＭ１１０６に格納する。その後、演算処理回路１１０８の動作を開始する。この時、切り替え回路１１１２は、第１の形態になるよう接続されているものとする。演算処理回路１１０８は、ＲＡＭ１１０６の中に展開された書き換えプログラムの実行ステップに応じて動作する。この書き換えプログラムの中に、ＲＯＭ１１１５の中にあるデータチェック用のプログラムに制御を移す

ようなプログラムがあり、これを実行する。そして、演算処理回路１１０８の実行プログラムがＲＯＭ１１１５に移った後、接続切り替え回路１１１２を第２の形態になるように切り替える。

これにより、ＲＡＭ１１０６とデータを入出力するバス１１１４とが接続されるため、演算処理回路１１０８は、ＲＯＭ１１１５に格納されている、ＲＡＭ１１０６に展開された書き換えプログラムが正しいか否かを判断するプログラムに従い、ＲＡＭ１１０６のデータを読み込み、かつ正しいかどうかの判断をする。

正しいと判断されれば、ＲＯＭ１１１５に組み込まれている接続切り替え回路１１１２を第１の形態に戻すように切り替えるプログラムによって、接続切り替え回路１１１２は第１の状態に切り替られ、以後本来実行すべきプログラムを実行する。

なお、ＲＡＭ１１０６に格納されている書き換えプログラムが正しいか否かを確認する方法は、ＲＯＭ１１１５に実装されている方式によるが、この方式には、たとえばチェックサムなどが用いられる。しかしながら、必ずしも方式を限定するものではなく、データのある決められた固まり単位で正しいことが判定できればよいことは言うまでもない。

次に、ＲＡＭ１１０６を第１２図のような構成にした場合について説明する。

第１２図は、本発明の実施の形態６に係る半導体集積回路装置のＲＡＭ１１０６の例を示したものである。

図において、ａ２６００、ａ２６０１、ａ２６０２、ａ２６０３、ａ２６０４は、メモリアドレスを示しており、ａ２６００はＲＡＭ１１０６におけるスタートアドレスを示し、ａ２６０４はエンドアドレスを示す。また、右上がり斜線ハッチをつけて示すように、ａ２６０１はＲＡＭ１１０６の全容量のちょうど半分に位置する場所のアドレスを示している。また、右下がり斜線をつけて示すように、ａ２６０２はアドレスａ２６０１とエンドアドレスａ２６０４とであらわされた容量のちょうど半分に位置する場所のアドレスを示す。同様に、ａ２６０３はアドレスａ２６０２とエンドアドレスａ２６０４とであらわされる容量のちょうど半分に位置するアドレスを示している。

以上のようなＲＡＭ１１０６を用いた半導体集積回路装置１１０１の動作につ

いて説明する。

まず最初に、ＲＡＭ１１０６のアドレスａ２６００からａ２６０１までの部分にメモリ１１０２から復号化回路１１０５を通してデータをダウンロードする。そのあと、アドレスａ２６０１からａ２６０４までの領域にも、ＲＡＭ１１０２に格納されている先に展開したアドレスａ２６００からａ２６０１までのデータと全く同じデータを、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路１１１２を切り替えてＲＡＭ１１０６のデータを読み出す。この読み出し時に、アドレスａ２６００からとアドレスａ２６０１からとのそれぞれ等距離にあるものを順次アクセスし、得られたデータのビットごとの排他的論理和を取る。暗号が正しく解け、データパスに異常がなく、かつ、ＲＡＭ１１０６の格納域ビットに異常がなければ、この排他的論理和の結果は、あるデータと同じデータとの排他的論理和となるため、０になる。したがって、この手順を準次繰り返し、各排他的論理和が０であることを確かめれば、メモリ１１０２から復号化回路１１０５を通してＲＡＭ１１０６に正しく展開できているという判断ができる。上記手順を残り領域の１／２ずつ繰り返し実行することで、ＲＡＭ１１０６には、演算処理回路１１０８のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

このように、ＲＡＭ１１０６を上記構成にすることにより、何らかの不具合のために、上記手順の排他的論理和が０とならない場合には、ＲＡＭ１１０６に格納されているデータに不具合があると判断できるとともに、不具合発生アドレスも知ることができる。

なお、メモリ１１０２からＲＡＭ１１０６に展開するデータ量は、ＲＡＭ１１０６の書き換えプログラムが格納されていない領域の１／２以下ずつであればよいが、排他的論理和をとる上記方法においては、１／２が読み出し可能な最大データ量であるので、１／２とすることで書き込み効率を大きくとれる。

また、本実施の形態６において、このように構成されたＲＡＭ１１０６を用いて、データチェックプログラムＲＯＭ１１１５に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムＲＯＭ１１１５がない場合でも、実施の形態５のように、ダウンロードするプログラムに予

めデータチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

次に、メモリ１１０２の構成を第１３図のような構成にした場合について説明する。

第１３図は、本発明の実施の形態６に係る半導体集積回路装置におけるメモリ１１０２の例を示したものである。

図において、ａ２７１０、ａ２７１１、ａ２７１２、ａ２７１３、ａ２７１４、ａ２７１５、ａ２７１６、ａ２７１７は、メモリ１１０２におけるアドレスを示している。アドレスａ２７１0は、メモリ１１０２のスタートアドレスを示し、アドレスａ２７１７は、メモリ１１０２のエンドアドレスを示す。また、アドレスａ２７１０とアドレスａ２７１１に囲まれた空間には、第１２図で示したＲＡＭ１１０６のアドレスａ２６００からａ２６０１に入るべきデータを暗号化して格納する。便宜上これを「データＡ」と呼ぶ。また、アドレスａ２７１１とアドレスａ２７１２に囲まれた空間には、復号化回路１１０５によって復号化するとＲＡＭ１１０６のアドレスａ２６００からａ２６０１に入るべきデータ、即ち「データＡ」を各ビットごとに反転したものが得られるようなデータが格納される。これを便宜上「データＡ´」と呼ぶ。同様に、アドレスａ２７１２とアドレスａ２７１３に囲まれた空間には、ＲＡＭ１１０６のアドレスａ２６０１からａ２６０２に入るべきデータを暗号化したものを格納し、アドレスａ２７１３とアドレスａ２７１４に囲まれた空間には、復号化回路１１０５によって復号化するとＲＡＭ１１０６のアドレスａ２６０１からａ２６０２に入るべきデータを各ビットごとに反転したものが得られるようなデータが格納される。これらを便宜上それぞれ、「データＢ」「データＢ´」と呼ぶ。「データＣ」及び「データＣ´」も同様の対応である。このような手順を繰り返し、ＲＡＭ１１０６に格納すべき全てのプログラム及びその反転データを上記手順に従って、暗号化してメモリ１１０２に格納する。

以上のように構成されたメモリ１１０２、及びＲＡＭ１１０６を使った半導体集積回路装置１１０１の動作について説明する。

まず、ＲＡＭ１１０６のアドレスａ２６００からａ２６０１までの部分にメモ

リ１１０２から復号化回路１１０５を通して「データA」をダウンロードする。そのあと、上記手順にて述べたメモリ１１０２に格納されている今ダウンロードしたデータの反転データを暗号化したものである「データA´」を、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路１１１２を切り替えてRAM１１０６のデータを読み出す。この読み出し時に、アドレスａ２６００からとアドレスａ２６０１からとのそれぞれ等距離にあるものを順次アクセスし、得られたデータのビットごとの論理積を取る。暗号が正しく解け、データパスに異常がなく、かつ、RAM１１０６の格納域ビットに異常がなければ、この論理積の結果は、あるデータとその反転データとの論理積となるため、０になる。したがって、この手順を順次繰り返し、各論理積が０であることをたしかめれば、メモリ１１０２から復号化回路１１０５を通してRAM１１０６に正しく展開できているということになる。メモリ１１０２には、RAM１１０６の各手順における残りの領域の１／２ずつのデータとその反転データが暗号化されて「データB」「データB´」「データC」「データC´」などのように対になって必要な量だけ格納されており、上記手順を残り領域の１／２づつデータがなくなるまで繰り返し実行することで、RAM１１０６には、演算処理回路１１０８のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

これにより、もしも何らかの不具合のために、上記手順の論理積が０とならない場合に、RAM１１０６に格納されているデータに不具合があると判断できるとともに、不具合発生アドレスも知ることができる。また、何らかの理由により、復号化回路１１０５に不具合がありRAM１１０６への出力が固定値になっていても、RAM２５０６に格納されているデータを上記手順で論理積をとれば、あるデータと同じデータの論理積であるため、０にはならない。このことで、正しくデータが格納されてはいないと判断できる。

なお、メモリ１１０２からRAM１１０６に展開するデータ量は、該RAM１１０６の残り領域の１／２以下ずつであってもよいが、論理積をとる上記方法においてはRAM１１０６の残り領域の１／２が読み出し可能な最大データ量であるので、１／２とすることで書き込み効率を大きくとれる。

また、本実施の形態６において、このように構成されたメモリ１１０２を用いて、データチェックプログラムＲＯＭ１１１５に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムＲＯＭ１１１５がない場合でも、実施の形態５のように、ダウンロードする書き換えプログラムに予めチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

以上のような本発明の実施の形態６に係る半導体集積回路装置は、ＲＡＭ１１０６に格納されている書き換えプログラムが正しく格納されているか否かを確認するためのチェックプログラムをＲＯＭ化したメモリ１１１５に格納したので、チェックプログラムの転送や、展開に誤りが発生しても、ＲＡＭ１１０６に格納された書き換えプログラムが正しく格納できたか否かの確認を、容易に、かつ、安定して行うことができる。

また、ＲＡＭ１１０６の書き換えプログラムが格納されていない領域を２分割した各々の領域に、該書き換えプログラムが格納されていない領域の１／２に相当するプログラムデータと、該１／２の領域に読み出したプログラムデータと同じデータとを順次読み出し、該読み出したそれぞれのデータから排他的論理和をとる手順を繰り返し行うようにしたので、ＲＡＭ１１０６に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、書き換えプログラムがＲＡＭ１１０６に正しく格納できていない場合に、ＲＡＭ１１０６における正しく格納できていない場所の情報を得ることができる。

また、ＲＡＭ１１０６の書き換えプログラムが格納されていない領域を２分割した各々の領域に、該書き換えプログラムが格納されていない領域の１／２に相当するプログラムデータと、該１／２の領域に読み出したプログラムデータを反転したデータとを順次読み出し、該読み出したそれぞれのデータから論理積をとる手順を繰り返し行うようにしたので、ＲＡＭ１１０６に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、何らかの理由により復号化回路１１０５の不具合でＲＡＭ１１０６への出力が固定値になり、排他的論理和をとってもデータが一致し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、Ｒ

ＡＭ１１０６に格納したプログラムの正誤を正しく判別できる。

なお、本発明の実施の形態１～６に係る半導体集積回路装置では、予め暗号化した書き換えプログラムを、半導体集積回路内にダウンロードする例を説明したが、暗号化されていない書き換えプログラムを半導体集積回路内にダウンロードしても同様の効果が得られるのはいうまでもない。

（実施の形態７）

本発明の実施の形態７に係る半導体集積回路装置は、予め暗号化された書き換えプログラムをメモリに格納した半導体集積回路装置において、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納されたか否かを、該書き換えプログラムの機密性を保持しながら確認するために、上記暗号化された書き換えプログラムを復号してＲＡＭに格納した後、該書き換えプログラムを再度暗号化し、該再度暗号化したプログラムデータと、上記予め暗号化されたプログラムデータとを比較するようにしたものである。

第１４図は、本発明の実施の形態７に係る半導体集積回路装置の構成を示す図である。

図において、１４０１は暗号化された書き換えプログラムをもつ半導体集積回路装置であり、１４０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、１４０３は制御用のマイコンである。半導体集積回路１４１１は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）１４０５と、復号化回路で復号された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）１４０６と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ１４０７の処理を行う演算処理回路（演算処理ユニット）１４０８と、上記ＲＡＭ１４０６に転送されたデータを再度暗号化する暗号化回路（暗号化手段）１４１０とから構成される。

次に、以上のように構成された半導体集積回路装置１４０１の動作を説明する。

まず、あらかじめ暗号化されメモリ１４０２に格納された書き換えプログラムを制御用マイコン１４０３の制御のもと、復号化回路１４０５をとおして復号しながらＲＡＭ１４０６に格納する。そして、メモリ１４０２に格納されたデータのうち、あらかじめ決められたデータ量の転送が終了した時点で、今度は、制御

用マイコン１４０３の制御のもと、今復号化してメモリ１４０６に格納した書き換えプログラムを読み出し、暗号化回路１４１０を通して再度暗号化し、該再度暗号化したプログラムデータとメモリ１４０２に格納されている予め暗号化したプログラムデータとを比較する。この両者のデータが一致すれば、最初にメモリ１４０２から読み出し、復号化回路１４０５にて復号化し、ＲＡＭ１４０６に格納した書き換えプログラムが、正しいと判断できる。

以上のような、本発明の実施の形態７に係る半導体集積回路装置は、予め暗号化したプログラムを半導体集積回路１４１１にダウンロードする半導体集積回路装置において、暗号化した書き換えプログラムを復号化し、ＲＡＭ１４０６に格納した後、暗号化回路１４１０で再度暗号化し、予め暗号化した書き換えプログラムと再度暗号化した書き換えプログラムとを比較するようにしたので、第三者に漏洩したくない機密情報の書き換えプログラムをそのまま外部に読み出すことなく、ＲＡＭ１４０６に格納した書き換えプログラムが正しく格納できたか否かを確認することができる。

（実施の形態８）

本発明の実施の形態８に係る半導体集積回路装置は、ＲＡＭに格納した書き換えプログラムが正しくないと判定された場合、該書き換えプログラムの修正箇所を検出して書き換えプログラムを修正可能にしたものである。

以下、本発明の実施の形態８に係る半導体集積回路装置を、第１５図、第１６図、及び第１７図を用いて説明する。

第１５図は、本発明の実施の形態８に係る半導体集積回路装置の構成を示した図であり、実施の形態７で説明した半導体集積回路装置において、ＲＡＭに格納されたプログラムが正しくないと判断された場合、プログラムを修正可能とする例を示したものである。

図において、１５００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、１５０３はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、１５０１は制御用のマイコンである。半導体集積回路１５０９は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）１５０２と、復号化回路１

５０２で復号された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）１５０４と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ１５０８の処理を行う演算処理回路（演算処理ユニット）１５０５と、ＲＡＭ１５０４に格納された書き換えプログラムを再度暗号化する暗号化回路１５０６とから構成される。ここまでの構成は第１４図の半導体集積回路装置１４０１と同じであるが、半導体集積回路装置１５００においては、暗号化回路１５０６の出力Ｓ１５０６とあらかじめ暗号化された書き換えプログラムが格納されているメモリ１５０３の出力Ｓ１５０３とを比較し、ＲＡＭ１５０４に正しく格納されなかった場所を検出する比較器１５０７を備えている。

以上のように構成された半導体集積回路装置１５００について、以下にその動作を説明する。第１６図は、実施の形態８に係る半導体回路１５００の動作フローを示す。

まず、暗号化した書き換えプログラムを復号化回路１５０２で復号し（ステップＳ１６０１）、制御用マイコン１５０１にしたがい、復号化した書き換えプログラムをＲＡＭ１５０４に入力する（ステップＳ１６０２）。ステップＳ１６０２でＲＡＭ１５０４に入力した書き換えプログラムを暗号化回路１５０６で再度、暗号化し（ステップＳ１６０３）、ステップＳ１６０３で暗号化した書き換えプログラムとメモリ１５０３に保持している書き換えプログラムとを比較する（ステップＳ１６０４）。ステップＳ１６０４でのチェックで正しくない場合、制御用マイコン１５０１に従って、正しくない部分のＲＡＭのビットを使用しないように書き換えプログラムを修正する（ステップＳ１６０５）。そして、ステップＳ１６０５で修正したプログラムを復号化し（ステップＳ１６０６）、該復号化したプログラムをＲＡＭ１５０４に入力する（ステップＳ１６０７）。

また、ステップＳ１６０５の書き換えプログラム修正の動作は、例えば、第１７図のように、ＲＡＭ１５０４に格納された書き換えプログラムの正しくない部分が、例えばマシン語単位などあらかじめ決められた単位のアドレスＸＸからアドレスＸＸ´とすると、アドレスＸＸからアドレスＸＸ´に格納されるべきデータを修正プログラムとしてアドレスＹＹからアドレスＹＹ´に格納するようにする。このとき、修正プログラムに、アドレスＸＸまで読み出したときにアドレ

スＹＹにＪＵＭＰする命令プログラムと、次にアドレスＹＹ´まで読み出したときにアドレスＸＸ´にＪＵＭＰする命令プログラムとを組み込むように修正を行えばよく、このように修正を行うことにより、ＲＡＭ１５０４に格納されたプログラムの読み出しを正常に行うことができる。

これにより、上記方法によると、修正プログラムをＲＡＭ１５０４に入力した後、読み出してチェックすることによりＲＡＭ１５０４内の欠陥のあるビットを使わないようにできるため、ＲＡＭの有効活用ができる。

なお、本実施の形態８では、予め暗号化した書き換えプログラムを格納するメモリ１５０３からの出力Ｓ１５０３と復号した書き換えプログラムを再度暗号化する暗号化回路１５０６からの出力Ｓ１５０６とを比較した結果から、ＲＡＭ１５０４に正しく格納できなかった場所を検出して、書き換えプログラムを修正したが、上述した書き換えプログラムの修正は、ＲＡＭの欠陥位置を検出できれば可能であるので、実施の形態６で説明したメモリ、及びＲＡＭの構成により読み出したデータの排他的論理和、及び論理積をとってデータをチェックする例においても適用可能である。

以上のような、実施の形態８に係る半導体集積回路装置は、書き換えプログラムがＲＡＭに正しく格納されたか否かを確認した結果、ＲＡＭに正しく格納されなかった場合に、正しく書き込めていないＲＡＭのビットを使用しないように書き換えプログラムを修正して、ＲＡＭにダウンロードするので、ＲＡＭの一部のビットが正しく生成できていなくても、その他の部分に書き込んで、書き換えプログラムを正しく動作させることができ、ＲＡＭを有効に活用することができる。

なお、本発明の実施の形態１～８の半導体集積回路装置では、書き換えプログラムをメモリ（第１の格納手段）に格納して、半導体集積回路内にダウンロードしたが、半導体集積回路装置外部に書き換えプログラムを保持し、例えば、インターネット等の通信手段を用いて、半導体集積回路内にダウンロードしても同様の効果を得ることができるのはいうまでもない。

また、本発明の実施の形態１～８では、半導体集積回路装置を例にとって説明したが、半導体集積回路装置に相当するものが、外部からアクセス不可能な領域（格納手段）を有する半導体集積回路を搭載したシステムであってもよく、該シ

ステムのアクセス不可能な領域（格納手段）に対し機密データのダウンロードが成功したか否かを検証するデータ記憶検証装置（方法）であってもよく、同様の効果を得ることができるのはいうまでもない。

また、本発明の実施の形態２～８の半導体集積回路装置では、プログラムを格納するＲＡＭは外部からの読み出しが不可のものであることはいうまでもない。

産業上の利用可能性

以上のように、本発明にかかる半導体集積回路装置，データ記憶検証装置およびデータ記憶検証方法は、機密性を要するプログラムデータを外部に漏らすことなく、正しく半導体集積回路内にダウンロードできたか否かを確認でき、特に著作権保護が必要なプログラム等のダウンロードが成功したか否かを確認するのに適する。

請 求 の 範 囲

1． 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記第２の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、

上記第２の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第１の格納手段からの上記書き換えプログラムを、上記第２の格納手段の外部読出し不可能領域に格納するようにした、

ことを特徴とする半導体集積回路装置。

2． 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記第２の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えた、

ことを特徴とする半導体集積回路装置。

3． 請求の範囲第２項に記載の半導体集積回路装置において、

上記制御回路は、上記第２の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するものとした、

ことを特徴とする半導体集積回路装置。

4． 請求の範囲第２項に記載の半導体集積回路装置において、

上記制御回路は、上記第２の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとした、

ことを特徴とする半導体集積回路装置。

5． 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、

上記第２の格納手段に格納した上記書き換えプログラムの一部を実行する、

ことを特徴とする半導体集積回路装置。

6． 請求の範囲第５項に記載の半導体集積回路装置において、

上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである、

ことを特徴とする半導体集積回路装置。

7． 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第１の格納手段から上記第２の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えた、

ことを特徴とする半導体集積回路装置。

8． 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回

路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、

上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、

上記第２の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、

上記第２の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行う、

ことを特徴とする半導体集積回路装置。

９．　請求の範囲第８項に記載の半導体集積回路装置において、

上記第２の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとした、

ことを特徴とする半導体集積回路装置。

１０．　請求の範囲第９項に記載の半導体集積回路装置において、

上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用する、

ことを特徴とする半導体集積回路装置。

１１．　請求の範囲第８項に記載の半導体集積回路装置において、

上記第２の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次２分割した構成とし、該２分割した各々の領域に同じプログラムデータを格納するものであり、

上記チェックプログラムは、上記２分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、

前回の判定結果が正しいと判定されたときに、前回２分割した領域の一方の領域を、プログラムが格納されていない領域としてさらに２分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、

上記第２の格納手段に格納すべきプログラムすべてを順次格納する、

ことを特徴とする半導体集積回路装置。

１２．　請求の範囲第１１項に記載の半導体集積回路装置において、

上記第２の格納手段は、該第２の格納手段の上記書き換えプログラムが格納されていない領域を順次２分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとした、

ことを特徴とする半導体集積回路装置。

１３．　請求の範囲第１２項に記載の半導体集積回路装置において、

上記一意に得られるデータが、該プログラムデータの反転データである、

ことを特徴とする半導体集積回路装置。

１４．　請求の範囲第８項ないし１３のいずれかに記載の半導体集積回路装置において、

上記チェックプログラムを予め格納したＲＯＭ（Read Only Memory）を備え、

上記ＲＯＭにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行う、

ことを特徴とした半導体集積回路装置。

１５．　請求の範囲第１項ないし第１４項のいずれかに記載の半導体集積回路装置において、

上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、

上記第１の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第２の格納手段に復号化した上記書き換えプログラムを格納する、

ことを特徴とする半導体集積回路装置。

１６．　半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさ

せるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第１の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第２の格納手段に転送する復号化手段と、

上記第２の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、

上記暗号化手段で暗号化された書き換えプログラムと上記第１の格納手段に保持している暗号化された書き換えプログラムとを比較する、

ことを特徴とする半導体集積回路装置。

１７．　請求の範囲第１１項ないし第１３項、及び第１６項のいずれかに記載の半導体集積回路装置において、

上記第２の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第１の格納手段に保持した書き換えプログラムを修正可能とした、

ことを特徴とする半導体集積回路装置。

１８．　請求の範囲第１項ないし第１７項のいずれかに記載の半導体集積回路装置において、

当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能とした、

ことを特徴とする半導体集積回路装置。

１９．　任意のデータを外部からアクセス可能な領域に記憶させる手段と、

前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する手段と、

正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２０．　機密データを外部からアクセス不可能な領域に記憶させる手段と、

前記機密データの特定部分を外部に出力する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２１．　プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる手段と、

前記記憶されたプログラムを実行させ、結果を外部に出力する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２２．　検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第１の手段と、

前記検査プログラムを実行させ、結果を外部に出力する第２の手段と、

前記第２の手段の終了後、前記機密プログラムを実行させる第３の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２３．　機密データを外部からアクセス不可能な領域に記憶させる手段と、

前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、

前記演算の結果を外部に出力する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２４．　機密データを外部からアクセス不可能な第１の領域に記憶させる第４の手段と、

機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域に記憶させる第５の手段と、

前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２５．　請求項２４記載のデータ記憶検証装置において、

前記第６の手段の終了後に前記第１の領域の命令に制御を移す第７の手段をさらに備えた、

ことを特徴とするデータ記憶検証装置。

２６．　請求項２４記載のデータ記憶検証装置において、

前記第５の手段は、前記第１の領域に記憶されている機密データ内に存在する

命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

２７．　請求項２４記載のデータ記憶検証装置において、

前記第５の手段は、第３の領域に前記第４の手段による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

２８．　機密データを復号する手段と、

前記復号されたデータを外部からアクセス不可能な領域に記憶させる手段と、

前記記憶されたデータを暗号化する手段と、

前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

２９．　機密プログラムを外部からアクセス不可能な領域に記憶させる第２１の手段と、

前記記憶されたプログラムを読み出す第２２の手段と、

前記読み出されたプログラムを命令単位で正当性を判定する第２３の手段と、

正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域において空いている領域に記憶させる第２４の手段と、

前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる第２５の手段と、

正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる第２６の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

３０．　任意のデータを外部からアクセス可能な領域に記憶させる工程と、

前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、

正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる工程とを含む、

ことを特徴とするデータ記憶検証方法。

３１．　機密データを外部からアクセス不可能な領域に記憶させる工程と、

前記機密データの特定部分を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

３２．　プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる工程と、

前記記憶されたプログラムを実行させ、結果を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

３３．　検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第１の工程と、

前記検査プログラムを実行させ、結果を外部に出力する第２の工程と、

前記第２の工程の終了後、前記機密プログラムを実行させる第３の工程とを含む、

ことを特徴とするデータ記憶検証方法。

３４．　機密データを外部からアクセス不可能な領域に記憶させる工程と、

前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、

前記演算の結果を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

３５．　機密データを外部からアクセス不可能な第１の領域に記憶させる第４の工程と、

機密データの一部であり、前記第１の領域に記憶されている検査プログラムを第２の領域に記憶させる第５の工程と、

前記第２の領域に記憶されている検査プログラムを実行して、前記第１の領域の機密データの正当性を検査する第６の工程とを含む、

ことを特徴とするデータ記憶検証方法。

３６．　請求項３６記載のデータ記憶検証方法において、

前記第６の工程の終了後に前記第１の領域の命令に制御を移す第７の工程をさらに含む、

ことを特徴とするデータ記憶検証方法。

３７．　請求項３５記載のデータ記憶検証方法において、

前記第５の工程は、前記第１の領域に記憶されている機密データ内に存在する

命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

３８．　請求項３５記載のデータ記憶検証方法において、

前記第５の工程は、前記第３の領域に前記第４の工程による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

３９．　機密データを復号する工程と、

前記復号されたデータを外部からアクセス不可能な領域に記憶させる工程と、

前記記憶されたデータを暗号化する工程と、

前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する工程とを含む、

ことを特徴とするデータ記憶検証方法。

４０．　機密プログラムを外部からアクセス不可能な領域に記憶させる工程と、

前記記憶されたプログラムを読み出す工程と、

前記読み出されたプログラムを命令単位で正当性を判定する工程と、

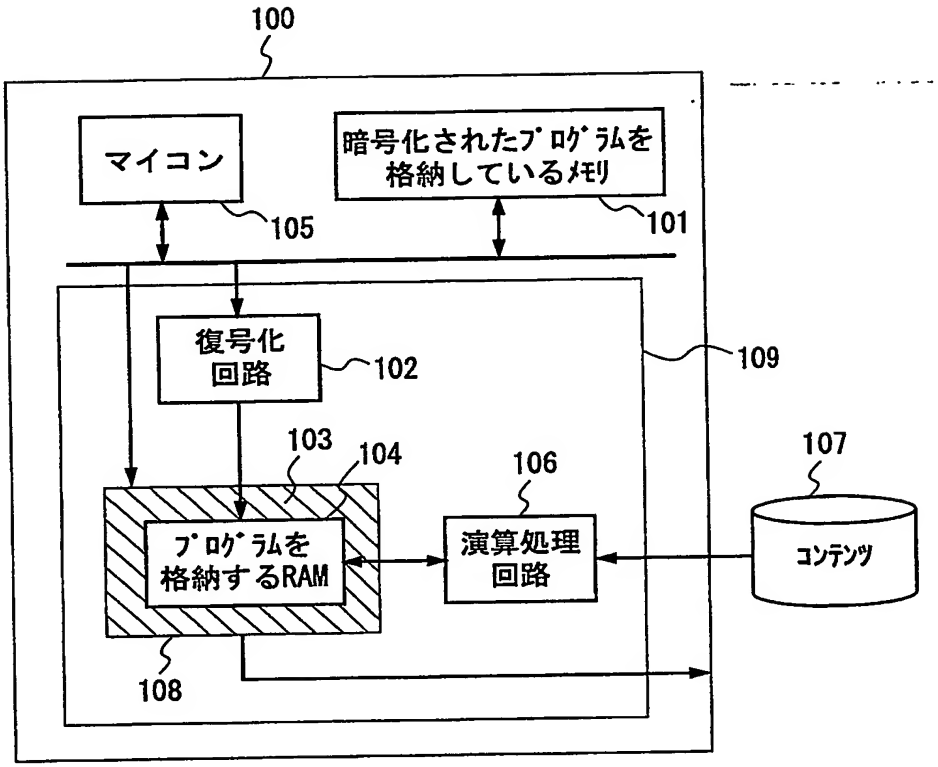
正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域において空いている領域に記憶させる工程と、

前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる工程と、

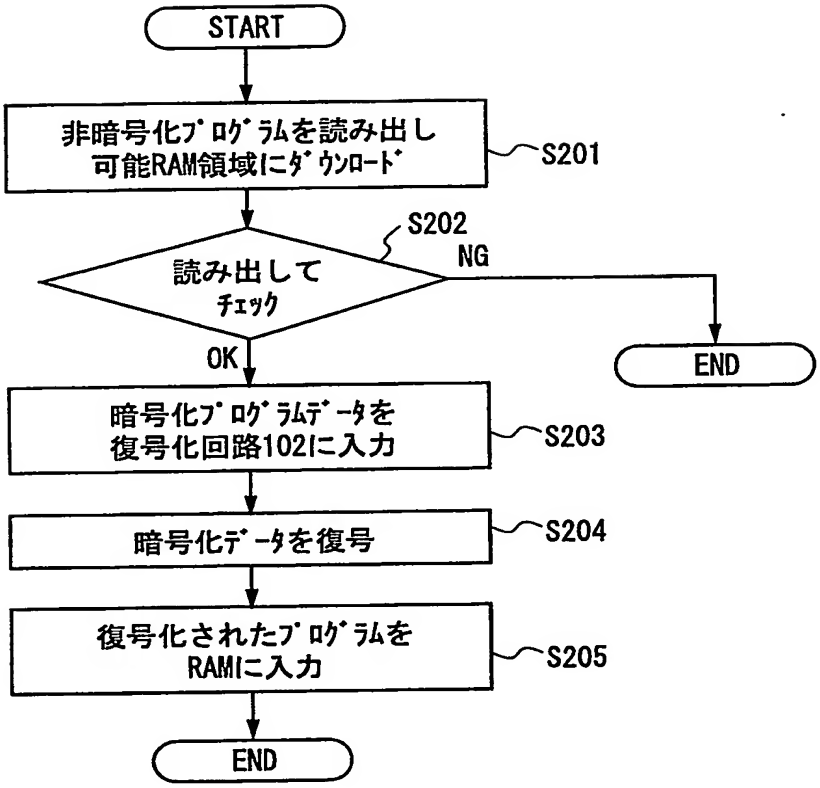
正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる工程とを含む、

ことを特徴とするデータ記憶検証方法。

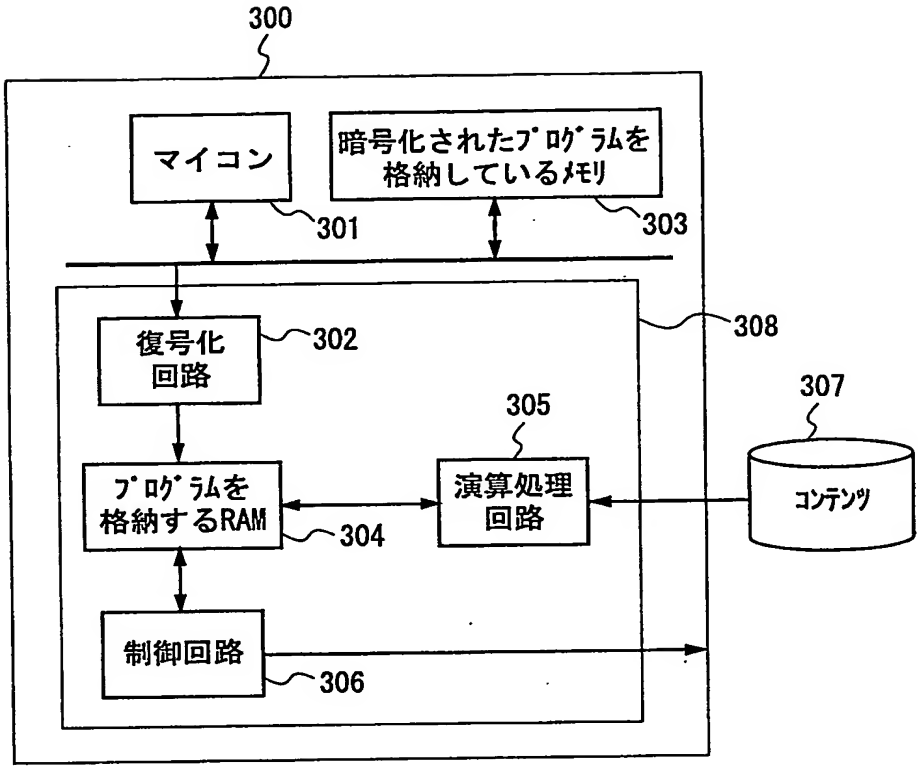
第1図


100
マイコン
105
暗号化されたﾌﾟﾛｸﾞﾗﾑを
格納しているﾒﾓﾘ
101
復号化
回路
102
109
103
104
106
107
ﾌﾟﾛｸﾞﾗﾑを
格納するRAM
演算処理
回路
ｺﾝﾃﾝﾂ
108

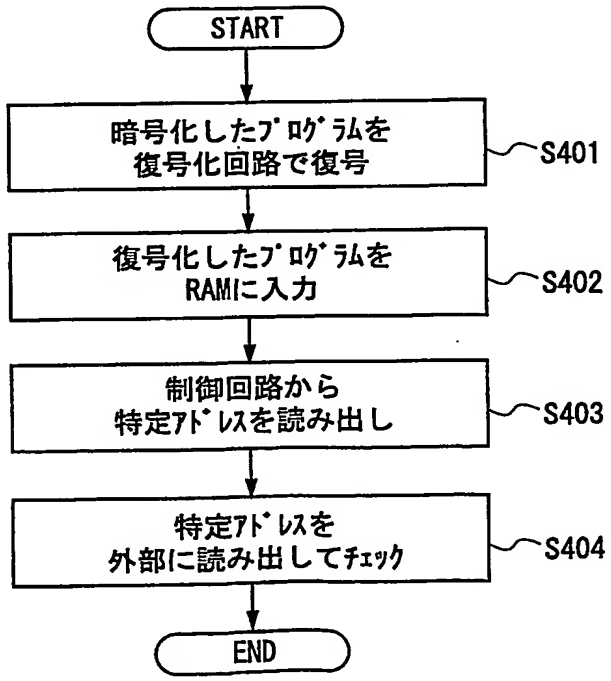
第2図


START
非暗号化ﾌﾟﾛｸﾞﾗﾑを読み出し
可能RAM領域にﾀﾞｳﾝﾛｰﾄﾞ
S201
S202
読み出して
ﾁｪｯｸ
NG
END
OK
暗号化ﾌﾟﾛｸﾞﾗﾑﾃﾞｰﾀを
復号化回路102に入力
S203
暗号化ﾃﾞｰﾀを復号
S204
復号化されたﾌﾟﾛｸﾞﾗﾑを
RAMに入力
S205
END

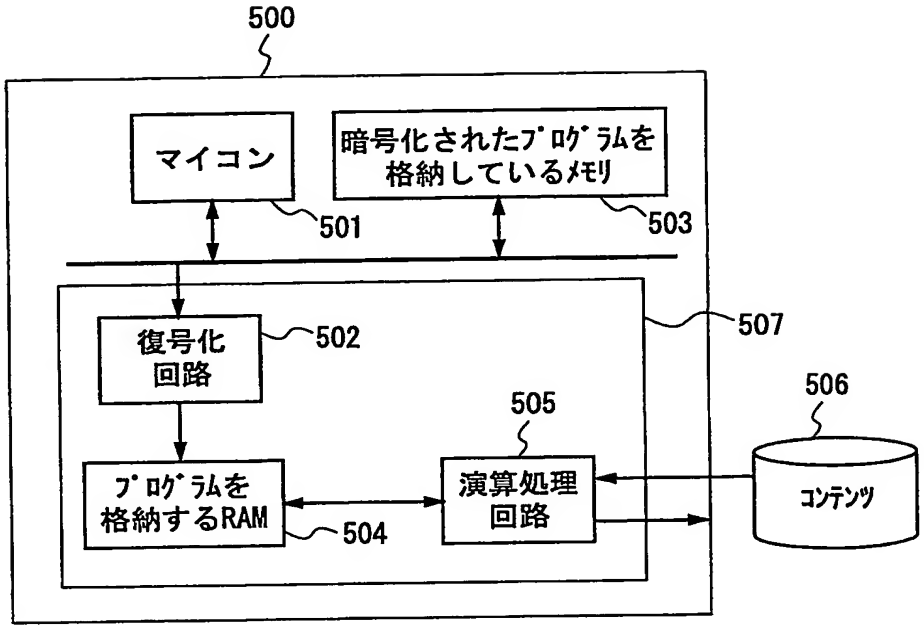
第3図


300
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
301
303
308
復号化回路
302
305
307
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
304
演算処理回路
ｺﾝﾃﾝﾂ
制御回路
306

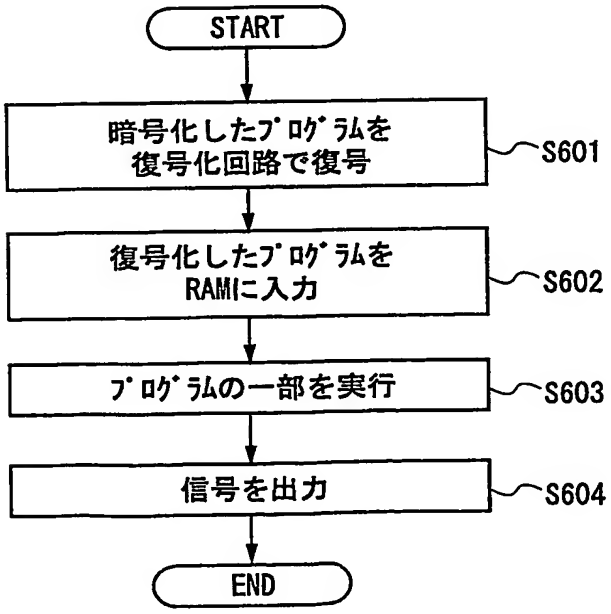
第4図


START
暗号化したﾌﾟﾛｸﾞﾗﾑを復号化回路で復号
S401
復号化したﾌﾟﾛｸﾞﾗﾑをRAMに入力
S402
制御回路から特定ｱﾄﾞﾚｽを読み出し
S403
特定ｱﾄﾞﾚｽを外部に読み出してﾁｪｯｸ
S404
END

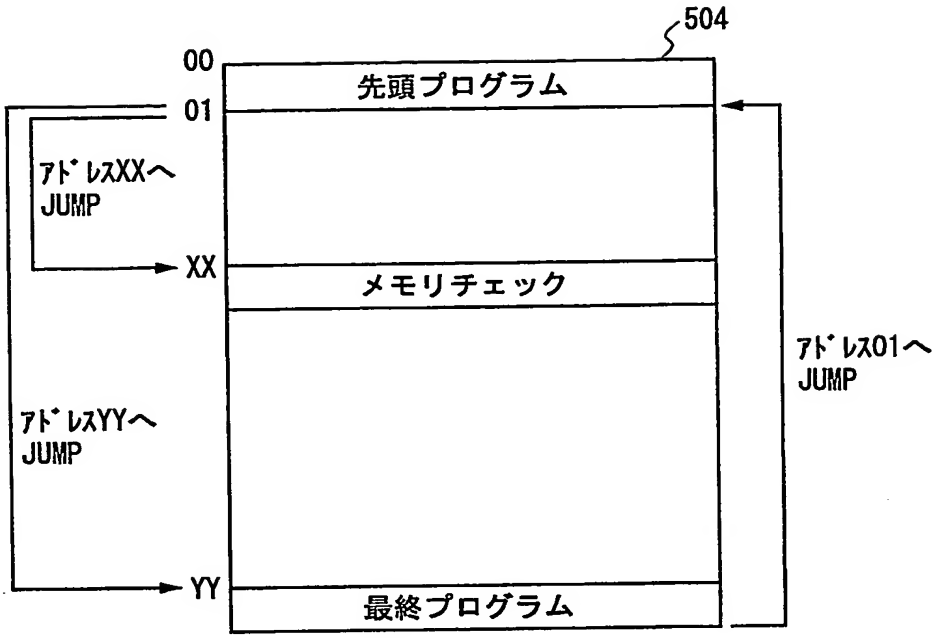
第5図


500
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを
格納しているﾒﾓﾘ
501
503
復号化
回路
502
507
506
505
ﾌﾟﾛｸﾞﾗﾑを
格納するRAM
504
演算処理
回路
ｺﾝﾃﾝﾂ

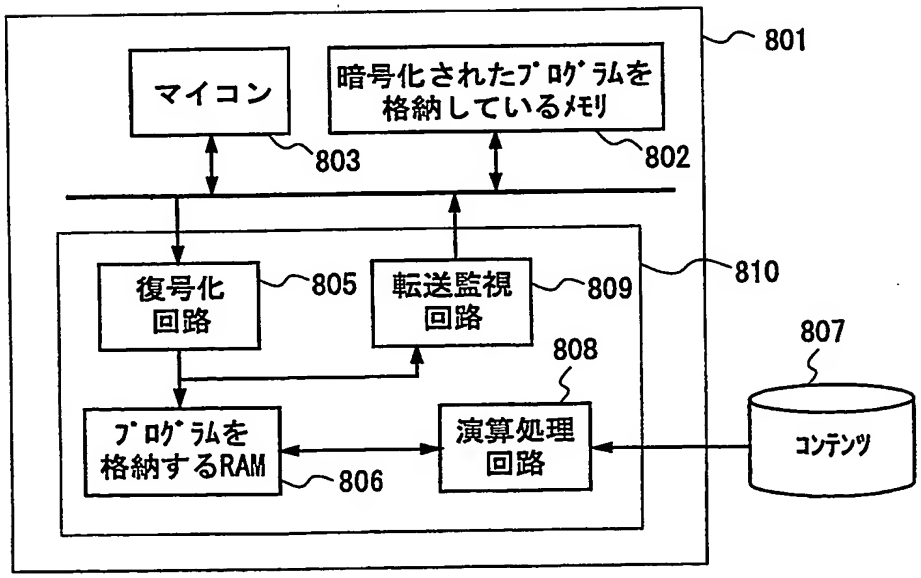
第6図


START
暗号化したﾌﾟﾛｸﾞﾗﾑを
復号化回路で復号
S601
復号化したﾌﾟﾛｸﾞﾗﾑを
RAMに入力
S602
ﾌﾟﾛｸﾞﾗﾑの一部を実行
S603
信号を出力
S604
END

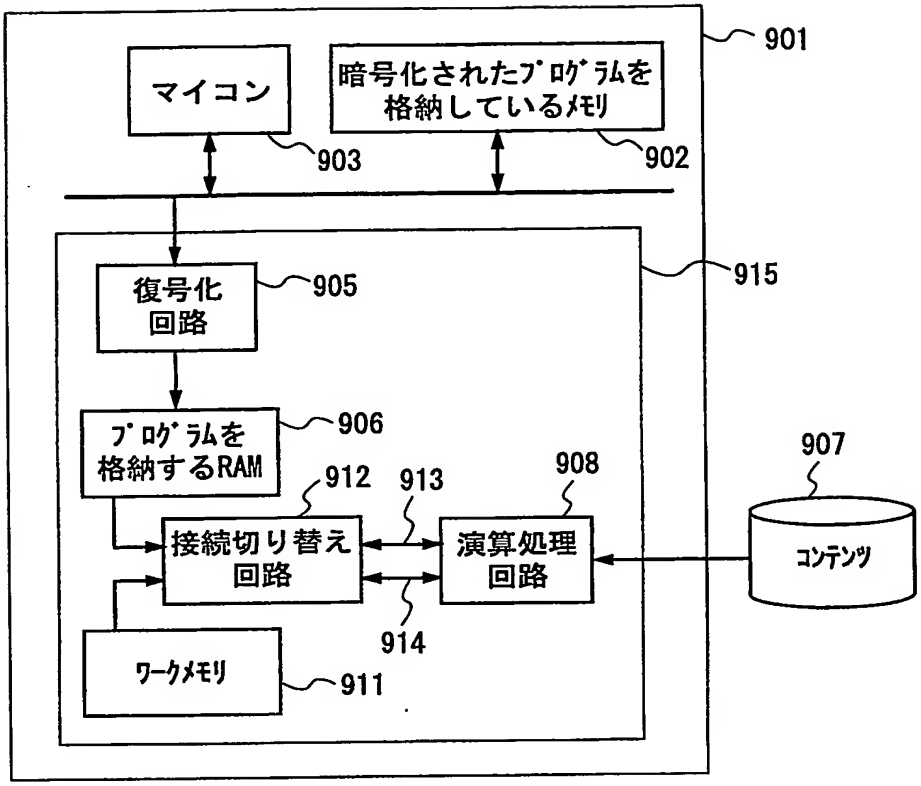
第7図


504
00
先頭プログラム
01
ｱﾄﾞﾚｽXXへ
JUMP
XX
メモリチェック
ｱﾄﾞﾚｽ01へ
JUMP
ｱﾄﾞﾚｽYYへ
JUMP
YY
最終プログラム

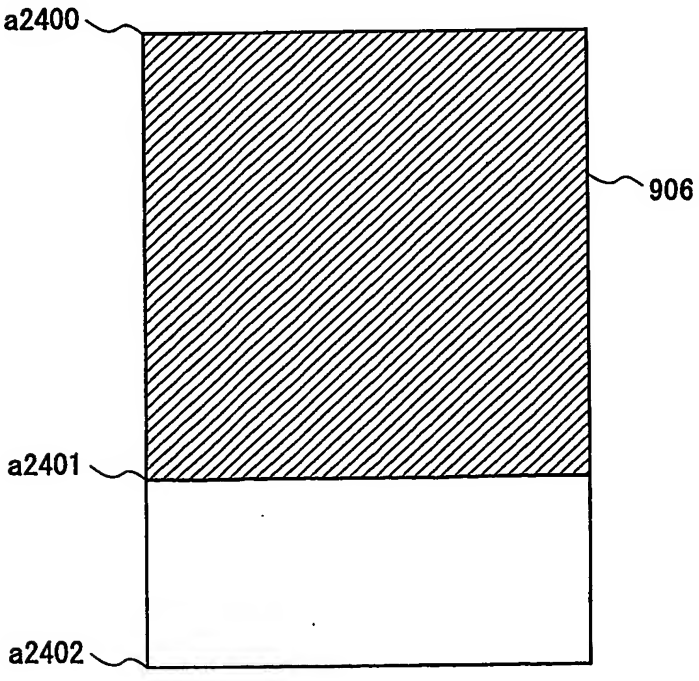
第8図


801
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを
格納しているﾒﾓﾘ
803
802
復号化
回路
805
転送監視
回路
809
810
807
808
ﾌﾟﾛｸﾞﾗﾑを
格納するRAM
806
演算処理
回路
ｺﾝﾃﾝﾂ

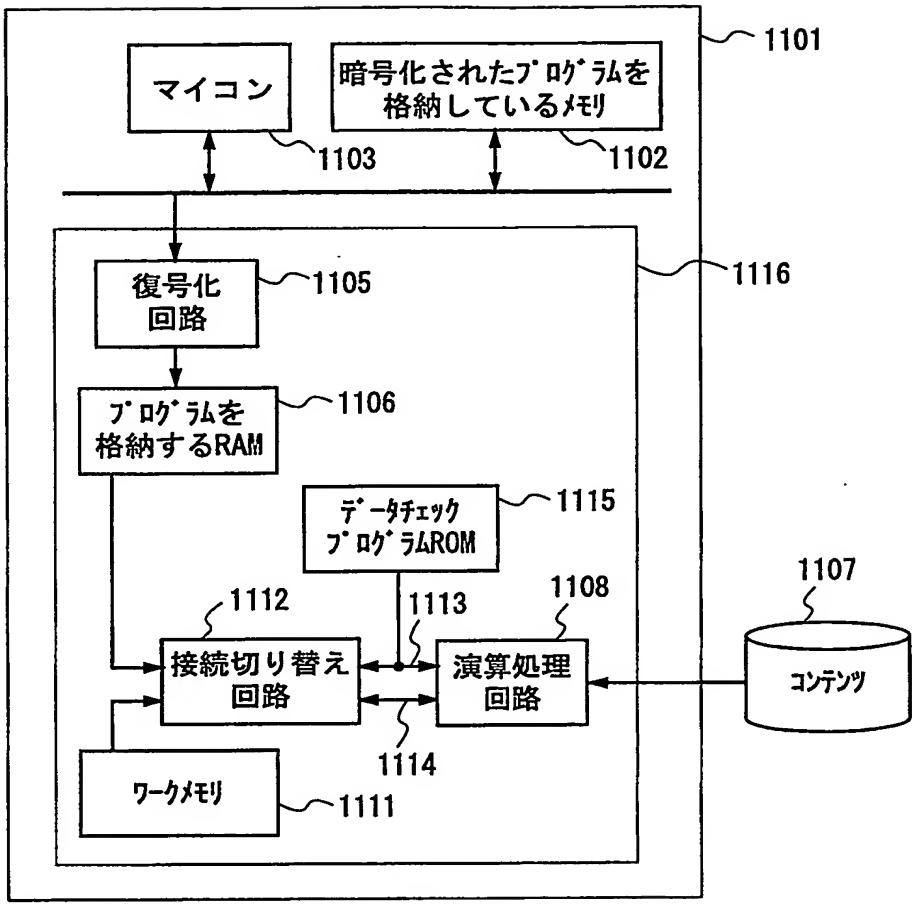
第9図


901
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
903
902
915
復号化回路
905
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
906
907
912
913
908
接続切り替え回路
演算処理回路
ｺﾝﾃﾝﾂ
914
ﾜｰｸﾒﾓﾘ
911

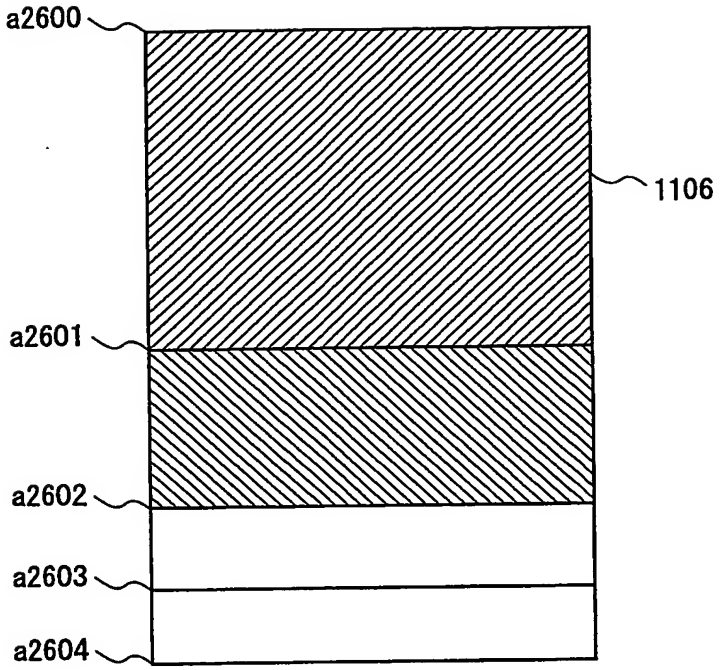
第10図


a2400
906
a2401
a2402

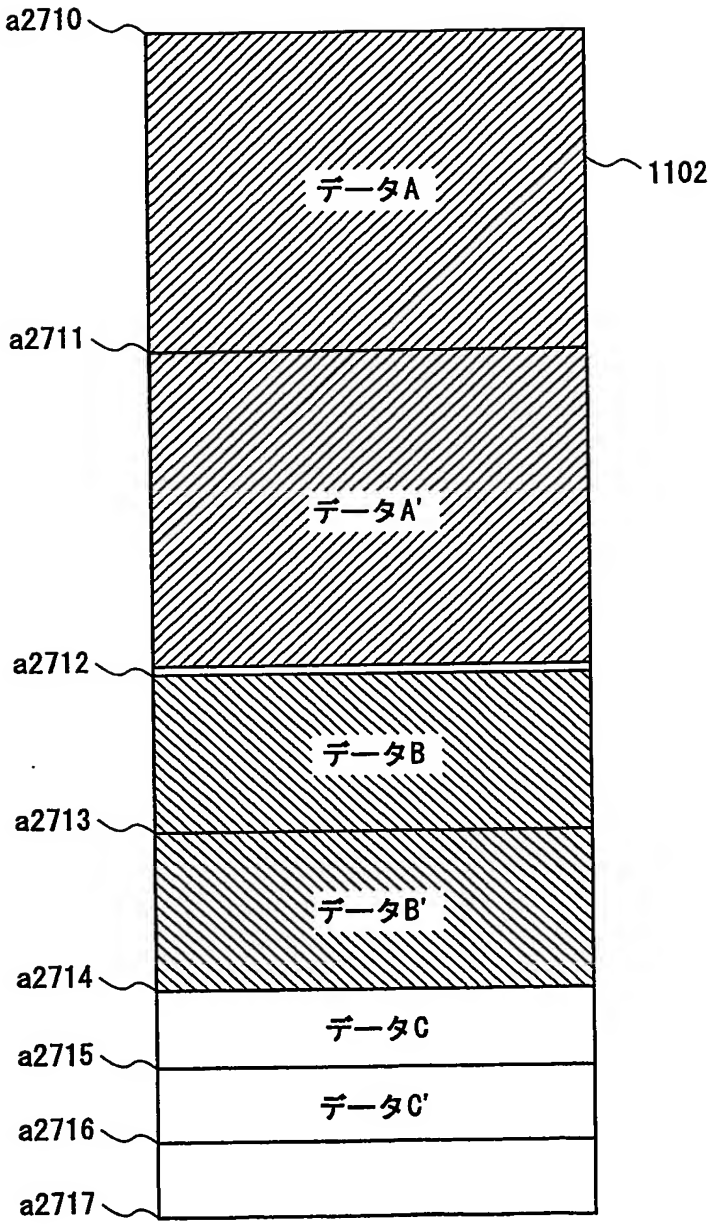
第11図


1101
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
1103
1102
1116
復号化回路
1105
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
1106
ﾃﾞｰﾀﾁｪｯｸﾌﾟﾛｸﾞﾗﾑROM
1115
1107
1112
1113
1108
接続切り替え回路
演算処理回路
コンテンツ
1114
ワークメモリ
1111

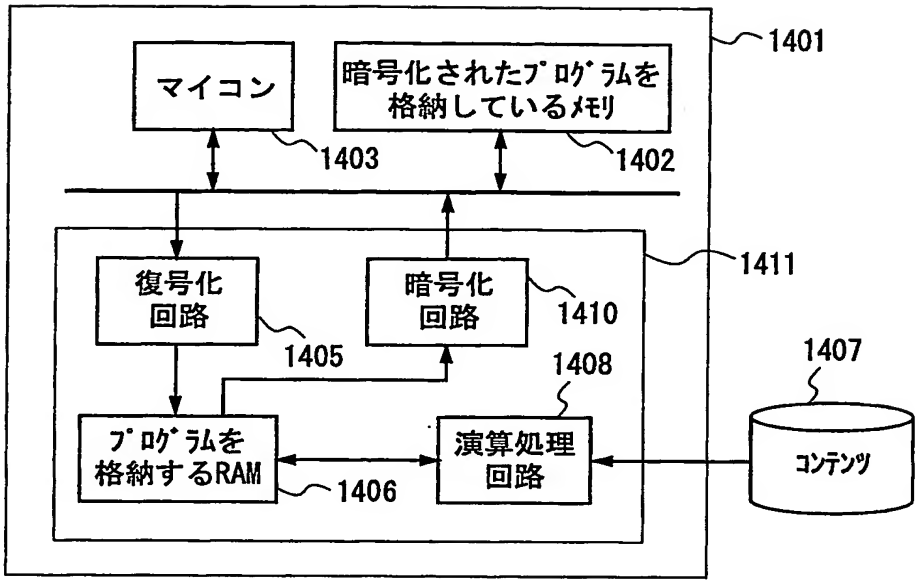
第12図



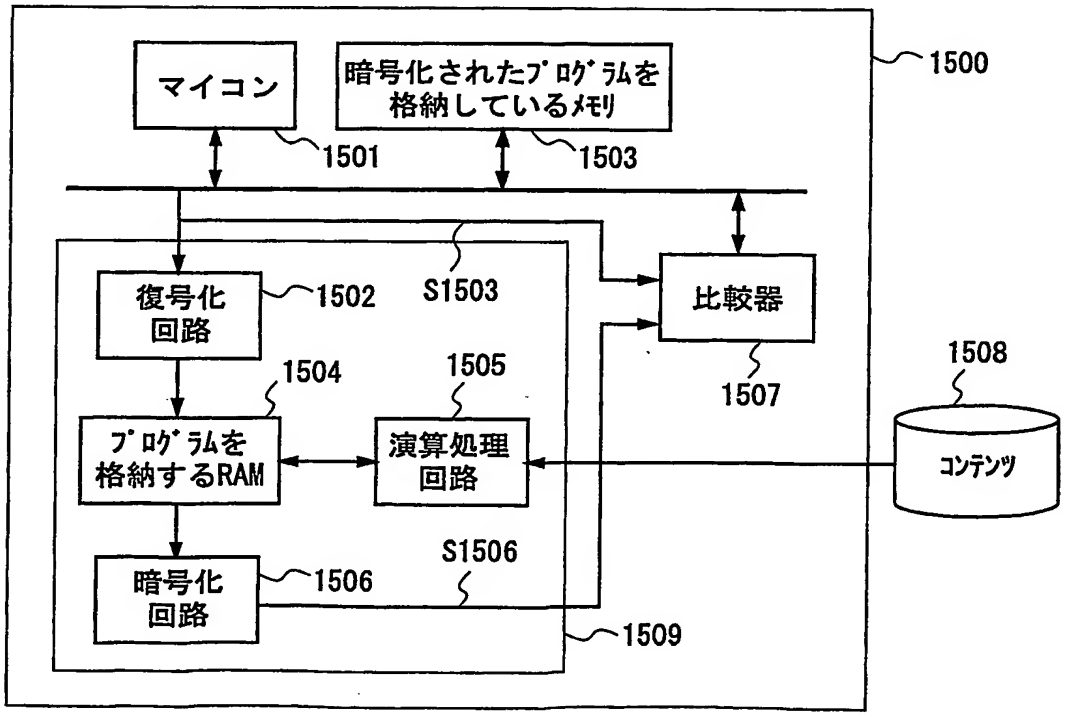
第13図


a2710
データA
1102
a2711
データA'
a2712
データB
a2713
データB'
a2714
データC
a2715
データC'
a2716
a2717

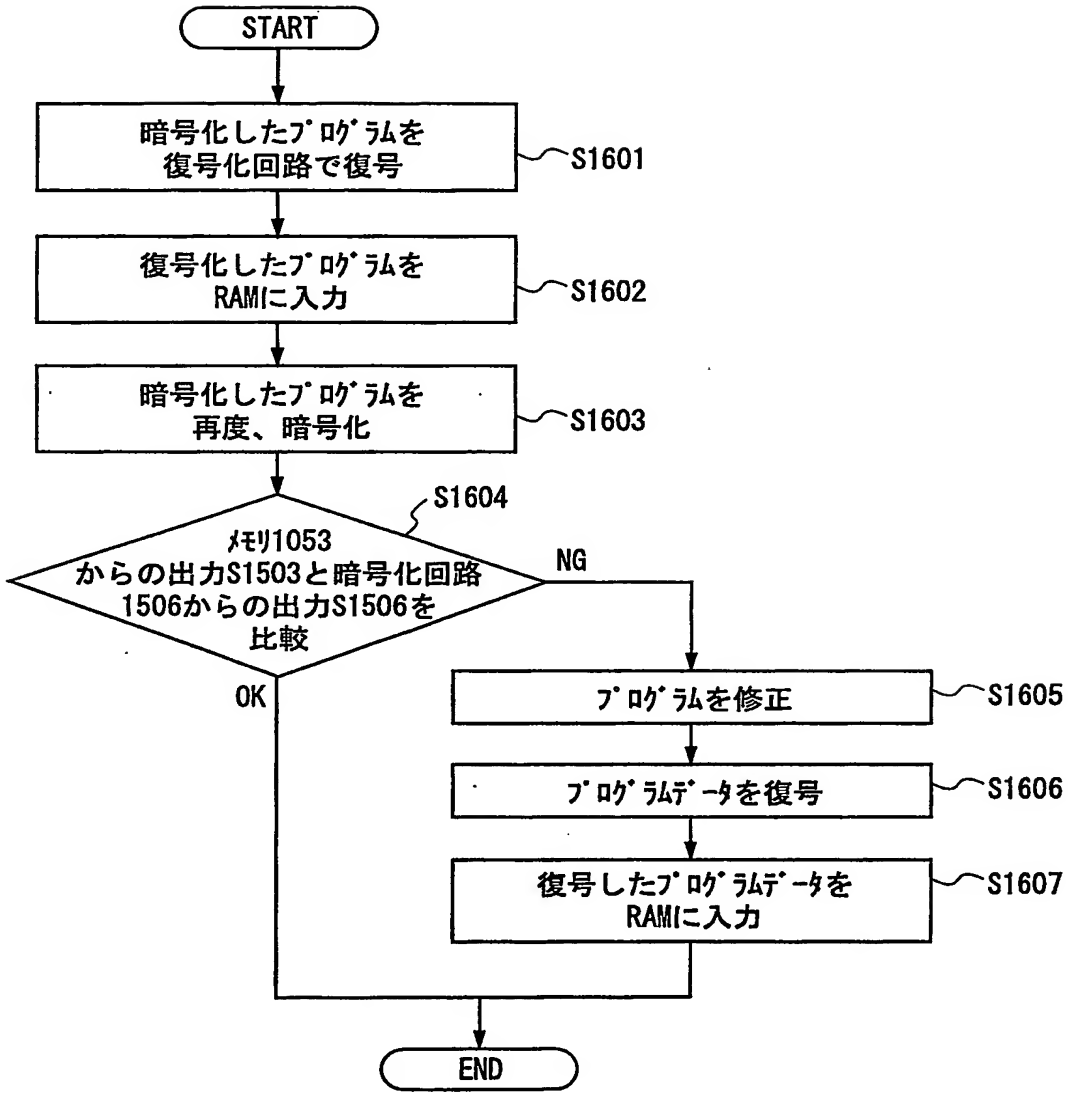
第14図


1401
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
1403
1402
1411
復号化回路
暗号化回路
1410
1405
1408
1407
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
演算処理回路
1406
ｺﾝﾃﾝﾂ

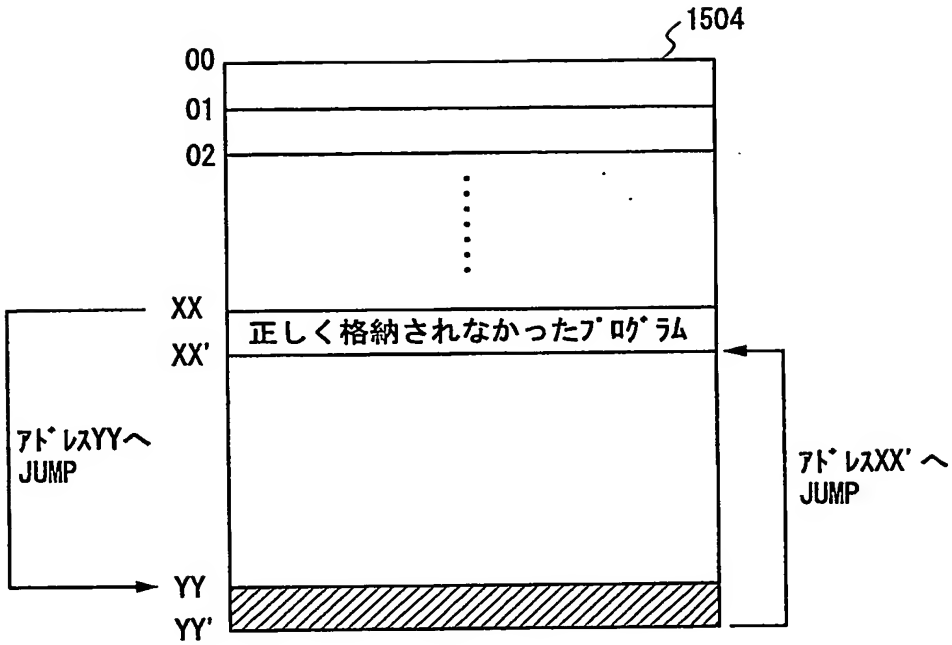
第15図


1500
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
1501
1503
復号化回路
1502
S1503
比較器
1504
1505
1507
1508
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
演算処理回路
ｺﾝﾃﾝﾂ
S1506
暗号化回路
1506
1509

第16図


START
暗号化したﾌﾟﾛｸﾞﾗﾑを
復号化回路で復号
S1601
復号化したﾌﾟﾛｸﾞﾗﾑを
RAMに入力
S1602
暗号化したﾌﾟﾛｸﾞﾗﾑを
再度、暗号化
S1603
S1604
ﾒﾓﾘ1053
からの出力S1503と暗号化回路
1506からの出力S1506を
比較
NG
OK
ﾌﾟﾛｸﾞﾗﾑを修正
S1605
ﾌﾟﾛｸﾞﾗﾑﾃﾞｰﾀを復号
S1606
復号したﾌﾟﾛｸﾞﾗﾑﾃﾞｰﾀを
RAMに入力
S1607
END

第17図


1504
00
01
02
XX
XX'
正しく格納されなかったﾌﾟﾛｸﾞﾗﾑ
ｱﾄﾞﾚｽYYへ
JUMP
ｱﾄﾞﾚｽXX'へ
JUMP
YY
YY'

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/07541

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F1/00, G06F9/06, G06F12/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1926-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 5-66937 A (Oki Electric Industry Co., Ltd.), 19 March, 1993 (19.03.93), All pages; all drawings (Family: none)	2-14 15-19,22-30, 33-40 1
X Y A	JP 2000-148502 A (NEC Corp.), 30 May, 2000 (30.05.00), All pages; all drawings (Family: none)	2-14 15-19,22-30, 33-40 1
X Y A	JP 10-11279 A (Tamura Electric Works, Ltd.), 16 January, 1998 (16.01.98), All pages; all drawings (Family: none)	2-14 15-19,22-30, 33-40 1

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 04 September, 2003 (04.09.03)	Date of mailing of the international search report 16 September, 2003 (16.09.03)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/07541

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 62-67800 A (Hitachi, Ltd.), 27 March, 1987 (27.03.87), All pages; all drawings & EP 215464 A2 & US 4777586 A & US 4905142 A	21,32 19,22-28, 30,33-39
X Y	JP 63-186330 A (Anritsu Corp., Nippon Telegraph And Telephone Corp.), 01 August, 1988 (01.08.88), All pages; all drawings (Family: none)	21-23,32-34 19,24-28,30, 35-39
X Y	JP 7-105169 A (NEC Corp.), 21 April, 1995 (21.04.95), All pages; all drawings (Family: none)	21,32 19,22-28,30, 33-39 23,34
X Y	JP 11-282756 A (Nakamichi Corp.), 15 October, 1999 (15.10.99), All pages; all drawings (Family: none)	19,21,22, 24-28,30,33, 35-39
Y	JP 63-240629 A (Nicksdorf Computer AG.), 06 October, 1988 (06.10.88), All pages all drawings & EP 280035 A2 & US 5224160 A	15-18,28,39
Y	JP 6-259242 A (Hitachi, Ltd.), 16 September, 1994 (16.09.94), All pages; all drawings; particularly, Par. No. [0009] (Family: none)	29,40

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/07541

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☒ Claims Nos.: 20, 31
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
Claims 20 and 31 do not describe necessary matters and what is described is unclear. The description "secret data stored in area which cannot be accessed from outside" contradicts the description "a specific part of the secret data is output outside".

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Claim 1 relates to a technical feature used after a program stored in the second storage means is rewritten by the rewrite program stored in the first storage means and validity is checked, for storing the rewrite program in the external read out disabled area of the second storage means.
claims 2-6 relate to a technical feature for rewriting the program stored in the second storage means by the rewrite program stored in the first storage means and executing the rewritten program in the second storage means.

(continued to extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

Continuation of Box No.II of continuation of first sheet(1)

Claims 7-14, 16, 17, 28, and 39 relate to a technical feature for judging validity of the program when the program stored in the second storage means is rewritten by the rewrite program stored in the first storage means.

Claims 15 and 18 are not so linked as to form a single general inventive concept.

Claims 19 and 30 relate to a technical feature for storing arbitrary data in an area accessible from outside and when stored correctly, secret data is stored in an area inaccessible from outside.

Claims 21-27 and 32-38 relate to a technical feature for outputting only the program execution result stored in the area inaccessible from outside.

Claims 29 and 40 relate to a technical feature for judging program validity for each instruction and when the result is invalid, jump is performed to a valid program newly stored.

国際調査報[redacted]　　国際出願番号 [redacted]／ＪＰ０３／０７５４１

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl⁷　　G06F12/14, G06F1/00

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl⁷　　G06F12/14, G06F1/00, G06F9/06, G06F12/16

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926 - 1996
日本国公開実用新案公報　1971 - 2003
日本国登録実用新案公報　1994 - 2003
日本国実用新案登録公報　1996 - 2003

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 5-66937 A（沖電気工業株式会社） 1993.03.19，全頁，全図（ファミリーなし）	2-14
Y		15-19, 22-30, 33-40
A		1

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　04.09.03

国際調査報告の発送日　16.09.03

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　奥村　元宏　5N　3044

電話番号　０３－３５８１－１１０１　内線　３５８５

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2000-148502 A（日本電気株式会社） 2000.05.30，全頁，全図（ファミリーなし）	2-14
Y		15-19, 22-30, 33-40
A		1
X	JP 10-11279 A（株式会社田村電機製作所） 1998.01.16，全頁，全図（ファミリーなし）	2-14
Y		15-19, 22-30, 33-40
A		1
X	JP 62-67800 A（株式会社日立製作所） 1987.03.27，全頁，全図	21, 32
Y	& EP 215464 A2 & US 4777586 A & US 4905142 A	19, 22-28, 30, 33-39
X	JP 63-186330 A（アンリツ株式会社、日本電信電話株式会社） 1988.08.01，全頁，全図（ファミリーなし）	21-23, 32-34
Y		19, 24-28, 30, 35-39
X	JP 7-105169 A（日本電気株式会社） 1995.04.21，全頁，全図（ファミリーなし）	21, 32
Y		19, 22-28, 30, 33-39
X	JP 11-282756 A（ナカミチ株式会社） 1999.10.15，全頁，全図（ファミリーなし）	23, 34
Y		19, 21, 22, 24-28, 30, 33, 35-39
Y	JP 63-240629 A （ニクスドルフ・コンピュータ・アクチエンゲゼルシヤフト） 1988.10.06，全頁，全図 & EP 280035 A2 & US 5224160 A	15-18, 28, 39
Y	JP 6-259242 A（株式会社日立製作所） 1994.09.16，全頁，全図，特に【０００９】段落 （ファミリーなし）	29, 40

第Ⅱ欄の続き
請求の範囲１５及び１８は、単一の一般的発明概念を形成しているとはいえない。
請求の範囲１９及び３０は、任意のデータを外部からアクセス可能な領域に記憶し、正しく記憶された場合、外部からアクセス不可能な領域に機密データを記憶する技術に関するものである。
請求の範囲２１－２７及び３２－３８は、外部からアクセス不可能な領域に記憶されているプログラムの実行結果のみを外部に出力する技術に関するものである。
請求の範囲２９及び４０は、プログラムの正当性を命令毎に判断し、正当でないと判定された場合には新たに記憶した正当なプログラムのアドレスへジャンプする技術に関するものである。

国際調査報[redacted]　　国際出願番号 [redacted]T／ＪＰ０３／０７５４１

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☒ 請求の範囲 20,31 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
請求の範囲２０及び３１には、必要な事項が記載されておらず、また、その記載も著しく不明瞭である。「外部からアクセス不可能な領域に記憶された機密データ」及び「機密データの特定部分を外部に出力する」という記載は矛盾する。

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１は、第２の格納手段に格納されたプログラムを第１の格納手段に格納された書き換えプログラムにより書き換える際に、正当性の判定の後、書き換えプログラムを第２の格納手段の外部読出し不可能領域に格納する技術に関するものである。
請求の範囲２－６は、第２の格納手段に格納されたプログラムを第１の格納手段に格納された書き換えプログラムにより書き換えた後に、第２の格納手段の書き換えられたプログラムを実行する技術に関するものである。
請求の範囲７－１４，１６，１７，２８及び３９は、第２の格納手段に格納されたプログラムを第１の格納手段に格納された書き換えプログラムにより書き換える際に、プログラムの正当性の判定を行う技術に関するものである。

1．☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。